McAfee Email and Web Security Appliances (auf Intel-Hardware)

Installationshandbuch

COPYRIGHT

Copyright © 2010 McAfee, Inc. Alle Rechte vorbehalten.

Diese Publikation darf in keiner Form und in keiner Weise ohne die schriftliche Genehmigung von McAfee, Inc., oder ihren Lieferanten und angeschlossenen Unternehmen ganz oder teilweise reproduziert, übermittelt, übertragen, in einem Abrufsystem gespeichert oder in eine andere Sprache übersetzt werden.

MARKEN

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD sind eingetragene Marken oder Marken von McAfee, Inc. und/oder der Tochterunternehmen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit ist ein Merkmal der McAfee-Produkte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind alleiniges Eigentum der jeweiligen Besitzer.

INFORMATIONEN ZUR LIZENZ

Lizenzvereinbarung

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSEITE VERFÜGBAR IST, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN MCAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Inhaltsverzeichnis

Einführung in McAfee Email and Web Security Appliances 6

Verwendung dieses Handbuchs 6

Zielgruppe dieses Handbuchs 6

Definition der Begriffe in diesem Handbuch 7

Graphische Konventionen 8

Dokumentation 8

Verfügbare Ressourcen 8

Vorbereitung der Installation 10

Lieferumfang 10

Planen der Installation 11

Unangemessene Nutzung 11

Betriebsbedingungen 11

Positionieren der Appliance 11

Überlegungen zu Netzwerkmodi 12

Modus "Transparente Bridge" 13

Modus "Transparenter Router" 14

Modus "Expliziter Proxy" 16

Ausbringungsstrategien für die Verwendung des Geräts in einer DMZ 17

SMTP-Konfiguration in einer DMZ 18

Arbeitslastverwaltung 20

Anschließen und Konfigurieren der Appliance 21

Kurzanleitungstabelle für die Installation 21

Anschlüsse und Verbindungen 22

Montieren der Appliance 22

Montieren der Appliance in einem Rack 22

Verbindung mit dem Netzwerk 23

Port-Nummern 23

Verwenden von Kupfer-LAN-Verbindungen 23

Verwenden von Glasfaser-LAN-Verbindungen 24

Monitor und Tastatur 24

Anschließen der Appliance an das Stromnetz 24

Installieren der Software. 25
Verwenden der Konfigurationskonsole. 25
Begrüßungsseite. 26
Durchführen einer Standardinstallation. 26
Durchführen der benutzerdefinierten Einrichtung. 29
Wiederherstellung aus einer Datei. 36
Einrichten der Verwaltung durch ePO. 37
ePO-Einstellungen. 37
Grundlegende Einstellungen. 38
Netzwerkeinstellungen. 38
Cluster-Verwaltung. 39
Kennwort. 41
Zusammenfassung. 41
Testen der Konfiguration. 42
Kennenlernen der Benutzeroberfläche. 43
Testen des Geräts. 44
Verwenden des Geräts. 46
Updates und HotFixes. 46
Nach der Installation. 46
Funktionen der Appliance. **47**
Generieren von Berichten. 47
Verwenden von Richtlinien für die Verwaltung von Nachrichten-Scans. 48
Erstellen einer Antiviren-Scan-Richtlinie. 48
Erstellen einer Anti-Spam-Scan-Richtlinie. 49
Erstellen einer E-Mail-Compliance-Richtlinie. 50
Erstellen einer Richtlinie für die Inhaltsfilterung. 51
Informationen zum Verwalten virtueller Hosts. 52
Fehlerbehebung. **54**
Allgemeine Probleme. 54
Die Appliance wird nicht mit Strom versorgt. 54
Die Appliance empfängt keinen Datenverkehr aus dem Netzwerk. 54
Häufig gestellte Fragen. 55
Probleme mit der Benutzeroberfläche. 55
E-Mail-Probleme. 57
Zustellung. 57
E-Mail-Anhänge. 58
POP3. 59

Physische Konfiguration. 59
Systemkonfiguration. 60
Systemverwaltung. 60
Automatische Aktualisierung der Antiviren-Software. 60
Anti-Spam. 61
Weitere Hilfe – Die Link-Leiste. 63

Einführung in McAfee Email and Web Security Appliances

In diesem Handbuch erhalten Sie die notwendigen Informationen für die Installation der McAfee® Email and Web Security Appliance. Es erläutert die Schritte und die Verifikation des Installationsprozesses.

In diesem Handbuch wird beschrieben, wie Sie Email and Web Security Software konfigurieren. Wenn Sie diese Anweisungen befolgen, verfügen Sie über eine vollständig funktionsfähige Appliance.

Inhalt

- Verwendung dieses Handbuchs
- Definition der Begriffe in diesem Handbuch
- Graphische Konventionen
- Dokumentation
- Verfügbare Ressourcen

Verwendung dieses Handbuchs

In diesem Handbuch wird Folgendes behandelt:

- Planung und Ausführung Ihrer Installation.
- Umgang mit der Benutzeroberfläche.
- Testen der ordnungsgemäßen Funktion des Produkts.
- Anwendung der aktuellsten Erkennungsdefinitionsdateien.
- Vertrautmachen mit einigen Scan-Richtlinien, Erstellen von Berichten und Abrufen der Statusinformationen.
- Beheben einiger grundlegender Probleme.

Weitere Informationen zu den Scan-Funktionen des Produkts finden Sie in der Online-Hilfe.

Zielgruppe dieses Handbuchs

Dieses Handbuch richtet sich in erster Linie an Netzwerkadministratoren, die für das Virenschutz- und Sicherheitsprogramm ihres Unternehmens verantwortlich sind.

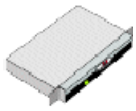
Definition der Begriffe in diesem Handbuch

In diesen Informationen werden einige der in diesem Handbuch häufig verwendeten Begriffe definiert.

Begriff	Beschreibung
Demilitarisierte Zone (DMZ)	Ein Computer-Host oder kleineres Netzwerk, das als Puffer zwischen ein privates Netzwerk und das äußere öffentliche Netzwerk eingefügt wurde, um den direkten Zugriff durch außenstehende Benutzer auf Ressourcen im privaten Netzwerk zu verhindern.
DAT-Dateien	Erkennungsdefinitionsdateien (DAT), auch als Signaturdateien bezeichnet, enthalten die Definitionen, die Viren, Trojaner, Spyware, Adware und andere potenziell unerwünschte Programme (PUPe) identifizieren, erkennen und entfernen.
Betriebsmodus	Es gibt drei Betriebsmodi für das Produkt: "Expliziter Proxy", "Transparente Bridge" und "Transparenter Router".
Richtlinie	Eine Sammlung der Sicherheitskriterien (z. B. Konfigurationseinstellungen, Benchmarks und Spezifikationen für den Netzwerkzugriff), die die erforderliche Compliance-Stufe für Benutzer, Geräte und Systeme definieren, die von einer McAfee-Sicherheitsanwendung bewertet oder erzwungen werden kann.
Reputationsdienst-Prüfung	Teil der Absenderauthentifizierung. Wenn ein Absender die Reputationsdienst-Prüfung nicht besteht, ist die Appliance so eingestellt, dass die Verbindung beendet und die Nachricht nicht zugelassen wird. Die IP-Adresse des Absenders wird zu einer Liste blockierter Verbindungen hinzugefügt und in Zukunft automatisch auf Kernel-Ebene blockiert.

Graphische Konventionen

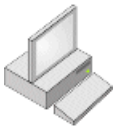
In den Abbildungen dieses Handbuches werden die folgenden Symbole verwendet.


Appliance

Internet

E-Mail-Server

Anderer Server (z. B. DNS-Server)


Benutzer- oder Client-Computer

Router

Switch

Firewall

Netzwerkzone (DMZ oder VLAN)

Netzwerk

Tatsächlicher Datenpfad

Wahrgenommener Datenpfad

Dokumentation

Dieses Handbuch ist im Lieferumfang Ihres Produkts enthalten. Weitere Informationen finden Sie in der zum Produkt gehörenden Online-Hilfe und der weiteren Dokumentation auf der Website http://mysupport.mcafee.com.

Verfügbare Ressourcen

Hier wird beschrieben, wo Sie weitere Informationen und Hilfe erhalten können.

McAfee-Produkte	McAfee-KnowledgeBase. Gehen Sie zu https://mysupport.mcafee.com/eservice/Default.aspx, und klicken Sie auf **Search the KnowledgeBase** (KnowledgeBase durchsuchen).
Produkthandbuch	McAfee-Download-Site. Enthält Informationen zu grundlegenden Konzepten, Richtlinien, Protokollen (SMTP, POP3, FTP, HTTP und ICAP), zur Wartung und Überwachung. Sie benötigen Ihre Grant-Nummer.
Online-Hilfe	Produktoberfläche. Enthält Informationen zu grundlegenden Konzepten, Richtlinien,

	Protokollen (SMTP, POP3, FTP, HTTP und ICAP), zur Wartung und Überwachung.

Vorbereitung der Installation

Um den sicheren Betrieb des Produkts zu gewährleisten, beachten Sie Folgendes, bevor Sie mit der Installation beginnen.

- Machen Sie sich mit den Betriebsmodi und den Funktionen vertraut. Es ist wichtig, dass Sie eine gültige Konfiguration auswählen.
- Entscheiden Sie, wie Sie die Appliance in Ihr Netzwerk integrieren möchten, und stellen Sie fest, welche Informationen Sie benötigen, bevor Sie beginnen. Sie benötigen beispielsweise den Namen und die IP-Adresse der Appliance.
- Packen Sie das Produkt so nah wie möglich am vorgesehenen Aufstellungsort aus.
- Nehmen Sie das Produkt aus der Schutzverpackung, und stellen Sie es auf eine ebene Fläche.
- Beachten Sie alle Sicherheitswarnungen.

VORSICHT: Lesen Sie alle mitgelieferten Sicherheitsinformationen, und machen Sie sich mit ihnen vertraut.

Inhalt

- Lieferumfang
- Planen der Installation
- Unangemessene Nutzung
- Betriebsbedingungen
- Positionieren der Appliance

Lieferumfang

Überprüfen Sie anhand der mit dem Produkt ausgelieferten Packliste, ob alle Komponenten enthalten sind.

Folgendes sollte vorhanden sein:

- Eine Appliance
- Netzkabel
- Netzwerkkabel
- Installations- und Wiederherstellungs-CD für Email and Web Security
- CD mit dem Linux-Quellcode

Wenn ein Element fehlt oder beschädigt ist, setzen Sie sich mit dem Händler in Verbindung.

- Vorbereitung der Installation

Planen der Installation

Beachten Sie Folgendes:

- Umgebungsanforderungen

  Informationen zu den Umgebungsanforderungen, einschließlich Temperatur, Belüftung und Platzbedarf.

- Stromanforderungen und Überlegungen

  Stromanforderungen und elektrische Faktoren, die vor der Installation bedacht werden müssen.

- Hardware-Spezifikationen und -Anforderungen
- Konfigurationsszenarien
- Vorbereitung der Installation

▸ Vorbereitung der Installation

Unangemessene Nutzung

Das Produkt ist:

- **Keine Firewall.** Es muss in Ihrer Organisation hinter einer ordnungsgemäß konfigurierten Firewall verwendet werden.
- **Kein Server zum Speichern zusätzlicher Software und Dateien.** Installieren Sie keine Software auf dem Gerät, und fügen Sie keine zusätzlichen Dateien hinzu, es sei denn, Sie werden in der Produktdokumentation oder von Ihrem Support-Mitarbeiter dazu aufgefordert. Das Gerät kann nicht alle Arten von Datenverkehr verarbeiten. Wenn Sie den Modus "Expliziter Proxy" verwenden, sollten nur Protokolle an das Gerät gesendet werden, die gescannt werden müssen.

▸ Vorbereitung der Installation

Betriebsbedingungen

Temperatur	10–35°C (50–95°F)
Luftfeuchtigkeit	20–80 % (nicht kondensierend) bei einem stündlichen Anstieg der Luftfeuchtigkeit von höchstens 10 %
Maximale Vibration	0,25 g bei 3–200 Hz (über 15 Minuten)
Maximale Erschütterung	Eine Stoßimpuls in der positiven Z-Achse (ein Impuls auf jeder Seite der Einheit) von 31 g für höchstens 2,6 ms
Höhe	-16 bis 3.048 m (-50 bis 10.000 Fuß)

Positionieren der Appliance

Installieren Sie die Appliance so, dass Sie den physischen Zugang zur Einheit steuern und auf die Anschlüsse und Verbindungen zugreifen können.

Im Lieferumfang der Appliance ist ein Set zur Montage in einem Rack enthalten, mit dem Sie die Appliance in einem 19-Zoll-Rack installieren können, wie unter Montieren der Appliance in einem Rack beschrieben.

Überlegungen zu Netzwerkmodi

Bevor Sie Ihre Email and Web Security Appliance installieren und konfigurieren, müssen Sie sich überlegen, welchen Netzwerkmodus Sie verwenden möchten. Vom ausgewählten Modus hängt es ab, wie Sie Ihre Appliance physisch an Ihr Netzwerk anschließen.

Sie können einen der folgenden Netzwerkmodi auswählen.

- **Modus "Transparente Bridge"** – Das Gerät fungiert als Ethernet-Bridge.
- **Modus "Transparenter Router"** – Das Gerät fungiert als Router.
- **Modus "Expliziter Proxy"** – Das Gerät fungiert als Proxy-Server und Mail-Relay.

Wenn Sie nach der Lektüre dieses und der folgenden Abschnitte weiterhin unsicher sind, welchen Modus Sie verwenden sollen, sprechen Sie mit einem Netzwerkexperten.

Architektonische Aspekte hinsichtlich der Netzwerkmodi

Hinsichtlich der Netzwerkmodi müssen Sie vor allem folgende Aspekte bedenken:

- Ob Kommunikationsgeräte die Existenz des Geräts kennen. Das heißt, ob das Gerät in einem der transparenten Modi arbeitet.
- Wie das Gerät physisch mit Ihrem Netzwerk verbunden wird.
- Die erforderliche Konfiguration zur Integration des Geräts in Ihr Netzwerk.
- An welchem Ort im Netzwerk die Konfiguration erfolgt.

Überlegungen vor dem Ändern des Netzwerkmodus

In den Modi "Expliziter Proxy" und "Transparenter Router" können Sie das Gerät so einrichten, dass es sich innerhalb mehrerer Netzwerke befindet. Dies wird durch das Einrichten mehrerer IP-Adressen für die LAN1- und LAN2-Anschlüsse ermöglicht.

Wenn Sie aus dem Modus "Expliziter Proxy" oder "Transparenter Router" in den Modus "Transparente Bridge" wechseln, wird nur die aktivierte IP-Adresse für jeden Anschluss übernommen.

TIPP: Nachdem ein Netzwerkmodus festgelegt wurde, empfiehlt es sich, diesen nicht mehr zu ändern, es sei denn, der Standort des Geräts ändert sich oder das Netzwerk wird neu strukturiert.

Inhalt

- Vorbereitung der Installation
- Modus "Transparente Bridge"
- Modus "Transparenter Router"
- Modus "Expliziter Proxy"

Modus "Transparente Bridge"

Im Modus "Transparente Bridge" bemerken die kommunizierenden Server das Gerät nicht. Der Betrieb des Geräts ist für die Server transparent.

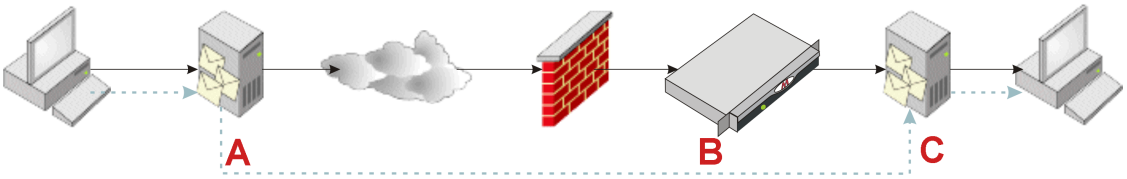


Abbildung 1: Transparente Kommunikation

In Abbildung 1: Transparente Kommunikation sendet der externe E-Mail-Server (**A**) E-Mails an den internen E-Mail-Server (**C**). Der externe Mail-Server kann nicht erkennen, dass die von ihm gesendete E-Mail-Nachricht vom Gerät abgefangen und gescannt wird (**B**).

Der externe E-Mail-Server scheint direkt mit dem internen E-Mail-Server zu kommunizieren (der Pfad wird als gestrichelte Linie dargestellt). Tatsächlich wird der Datenverkehr möglicherweise durch mehrere Netzwerkgeräte geleitet und vom Gerät abgefangen und gescannt, bevor er den internen Mail-Server erreicht.

Funktion des Geräts

Im Modus "Transparente Bridge" wird das Gerät über den LAN1- und den LAN2-Anschluss mit dem Netzwerk verbunden. Das Gerät scannt den empfangenen Datenverkehr und fungiert als Bridge, die zwei Netzwerksegmente verbindet, behandelt diese aber wie ein einziges logisches Netzwerk.

Konfiguration

Der Modus "Transparente Bridge" erfordert weniger Konfigurationsaufwand als die Modi "Transparenter Router" oder "Expliziter Proxy". Sie müssen nicht alle Clients, das Standard-Gateway, MX-Einträge, Firewall-NAT und E-Mail-Server neu konfigurieren, damit der Datenverkehr an das Gerät gesendet wird. Da das Gerät in diesem Modus nicht als Router fungiert, ist es auch nicht erforderlich, eine Routing-Tabelle zu aktualisieren.

Platzieren des Geräts

Aus Sicherheitsgründen sollten Sie das Gerät innerhalb Ihres Unternehmens und hinter einer Firewall betreiben.

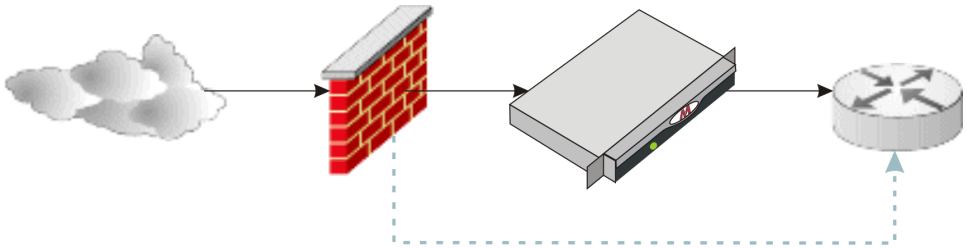


Abbildung 2: Einzelnes logisches Netzwerk

TIPP: Im Modus "Transparente Bridge" positionieren Sie das Gerät zwischen der Firewall und Ihrem Router, wie in Abbildung 2: Einzelnes logisches Netzwerk dargestellt.

In diesem Modus verbinden Sie zwei Netzwerksegmente physisch mit dem Gerät. Das Gerät behandelt diese als eine einzige logische Einheit. Da sich die Geräte – Firewall, Gerät und Router – im selben logischen Netzwerk befinden, müssen sie kompatible IP-Adressen im selben Subnetz haben.

Geräte auf der einen Seite der Bridge (z. B. ein Router), die mit den Geräten auf der anderen Seite der Bridge (z. B. einer Firewall) kommunizieren, bemerken die Bridge nicht. Sie erkennen nicht, dass der Datenverkehr abgefangen und gescannt wird. Deshalb wird dieser Betriebsmodus des Geräts als "Transparente Bridge" bezeichnet.

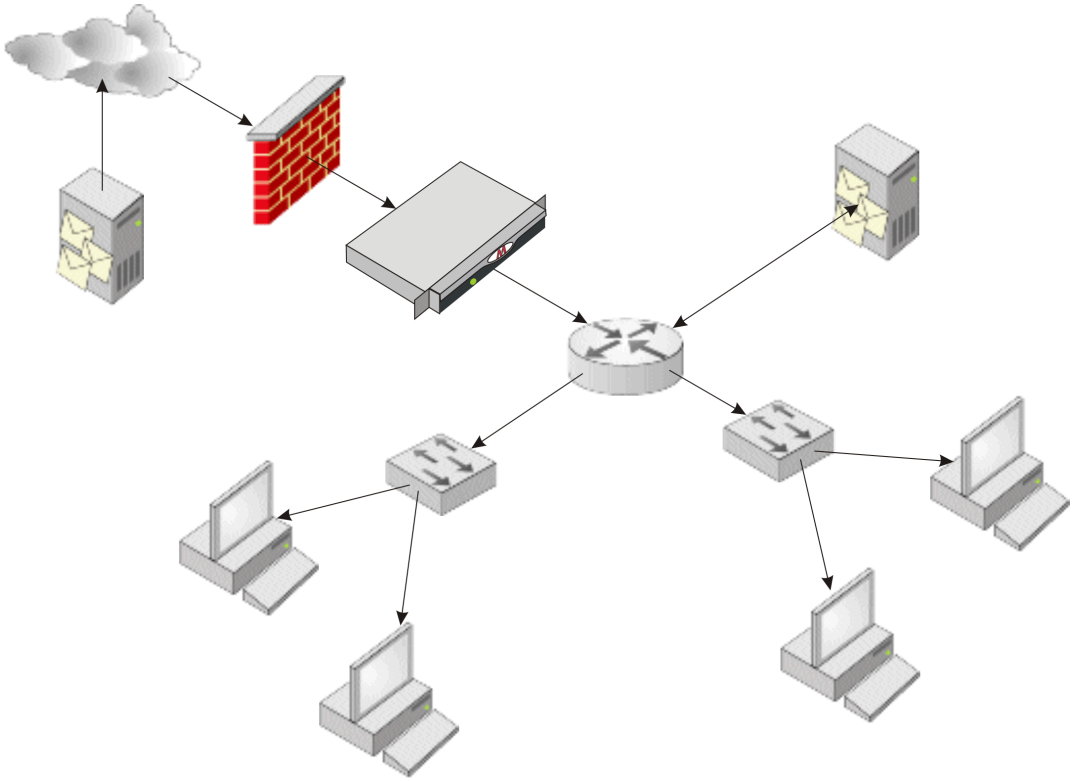


Abbildung 3: Modus "Transparente Bridge"

Modus "Transparenter Router"

Im Modus "Transparenter Router" scannt das Gerät den E-Mail-Verkehr zwischen zwei Netzwerken. Das Gerät hat eine IP-Adresse für ausgehenden gescannten Verkehr und muss eine IP-Adresse für eingehenden Verkehr haben.

Die kommunizierenden Netzwerkserver erkennen nicht, dass das Gerät zwischengeschaltet ist. Der Betrieb des Geräts ist für die Geräte *transparent*.

Funktion des Geräts

Im Modus "Transparenter Router" wird das Gerät mit den Netzwerken über den LAN1- und den LAN2-Anschluss verbunden. Das Gerät scannt den Datenverkehr, der über ein Netzwerk eingeht, und leitet ihn an das nächste Netzwerkgerät in einem anderen Netzwerk weiter. Das Gerät fungiert als Router (wobei es Datenverkehr zwischen den verschiedenen Netzwerken auf der Basis der Informationen in den Routing-Tabellen weiterleitet).

Konfiguration

Im Modus "Transparenter Router" müssen Sie Ihre Netzwerkgeräte nicht explizit neu konfigurieren, damit der Datenverkehr an das Gerät gesendet wird. Sie müssen lediglich die Routing-Tabelle für das Gerät konfigurieren und einige der Routing-Informationen für die Netzwerkgeräte auf einer Seite des Geräts ändern (der Geräte also, die an die LAN1- und LAN2-Anschlüsse des Geräts angeschlossen sind). Es könnte zum Beispiel erforderlich sein, das Gerät als Standard-Gateway zu konfigurieren.

Im Modus "Transparenter Router" muss das Gerät zwei Netzwerke miteinander verbinden. Das Gerät muss innerhalb Ihres Unternehmens hinter einer Firewall positioniert werden.

HINWEIS: Im Modus "Transparenter Router" werden weder Multicast-IP-Datenverkehr noch andere Protokolle wie NETBEUI und IPX (Nicht-IP-Protokolle) unterstützt.

Platzieren des Geräts

Verwenden Sie das Gerät im Modus "Transparenter Router", um einen im Netzwerk vorhandenen Router zu ersetzen.

TIPP: Wenn Sie den Modus "Transparenter Router" verwenden und keinen vorhandenen Router ersetzen, müssen Sie einen Teil Ihres Netzwerks neu konfigurieren, damit der Datenverkehr korrekt durch das Gerät fließt.

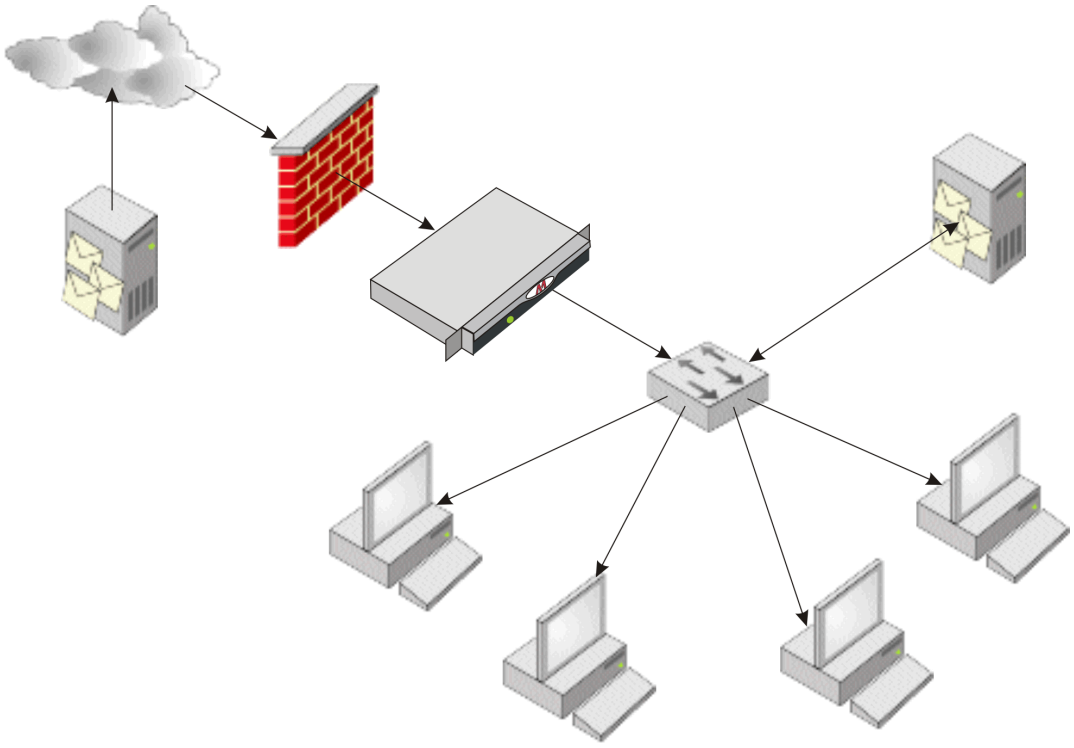


Abbildung 4: Konfiguration im Modus "Transparenter Router"

Sie müssen wie folgt vorgehen:

- Konfigurieren Sie die Client-Geräte so, dass sie auf das Standard-Gateway verweisen.
- Konfigurieren Sie das Gerät so, dass das Internet-Gateway als Standard-Gateway verwendet wird.
- Stellen Sie sicher, dass Ihre Client-Geräte E-Mails an die E-Mail-Server in Ihrem Unternehmen senden können.

Modus "Expliziter Proxy"

Im Modus "Expliziter Proxy" müssen einige Netzwerkgeräte so eingerichtet werden, dass sie Datenverkehr explizit an das Gerät senden. Das Gerät fungiert dann als Proxy oder Relay und verarbeitet den Datenverkehr für die Geräte.

Der Modus "Expliziter Proxy" ist am besten für Netzwerke geeignet, in denen Client-Geräte über ein einzelnes Upstream- und Downstream-Gerät eine Verbindung zum Gerät herstellen.

TIPP: Dies ist möglicherweise nicht die beste Option, wenn verschiedene Netzwerkgeräte erneut konfiguriert werden müssen, damit sie den Datenverkehr an das Gerät senden.

Netzwerk- und Gerätekonfiguration

Wenn sich das Gerät im Modus "Expliziter Proxy" befindet, müssen Sie den internen Mail-Server explizit so konfigurieren, dass er E-Mail-Verkehr an das Gerät sendet. Das Gerät prüft den E-Mail-Verkehr, bevor es ihn im Namen des Absenders an den externen Mail-Server weiterleitet. Der externe E-Mail-Server leitet die E-Mail dann an den Empfänger weiter.

Entsprechend muss das Netzwerk so konfiguriert werden, dass eingehende E-Mail-Nachrichten aus dem Internet nicht dem internen Mail-Server, sondern dem Gerät zugestellt werden.

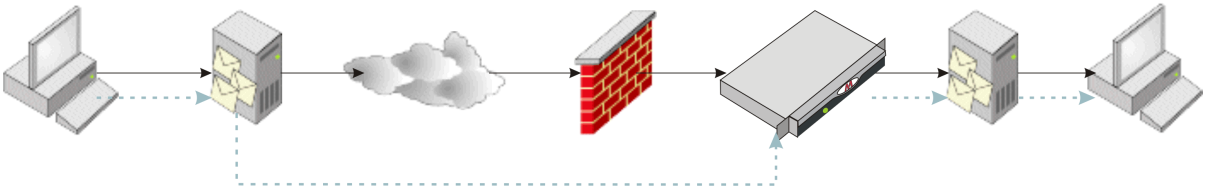


Abbildung 5: Weiterleiten des E-Mail-Verkehrs

Das Gerät kann den E-Mail-Verkehr dann prüfen, bevor es ihn im Namen des Absenders an den internen Mail-Server zur Zustellung weiterleitet, wie in Abbildung 5: Weiterleiten des E-Mail-Verkehrs dargestellt.

Beispielsweise kann ein externer Mail-Server direkt mit dem Gerät kommunizieren, auch wenn der Datenverkehr möglicherweise mehrere Netzwerkserver passiert, bevor er das Gerät erreicht. Der wahrgenommene Pfad verläuft vom externen Mail-Server zum Gerät.

Protokolle

Um ein unterstütztes Protokoll zu scannen, müssen Sie Ihre anderen Netzwerkserver oder Client-Computer so konfigurieren, dass das Protokoll durch das Gerät geleitet wird, sodass kein Datenverkehr das Gerät umgehen kann.

Firewall-Regeln

Im Modus "Expliziter Proxy" werden alle Firewall-Regeln, die für den Client-Zugriff auf das Internet eingerichtet wurden, außer Kraft gesetzt. Für die Firewall sind nur die IP-Adressinformationen für das Gerät sichtbar, nicht die IP-Adressen der Clients. Dies bedeutet, dass die Firewall ihre Internetzugriffsregeln nicht auf die Clients anwenden kann.

Platzieren des Geräts

Konfigurieren Sie die Netzwerkgeräte so, dass der zu scannende Datenverkehr an das Gerät gesendet wird. Das ist wichtiger als der Standort des Geräts.

Der Router muss allen Benutzern erlauben, eine Verbindung zum Gerät herzustellen.

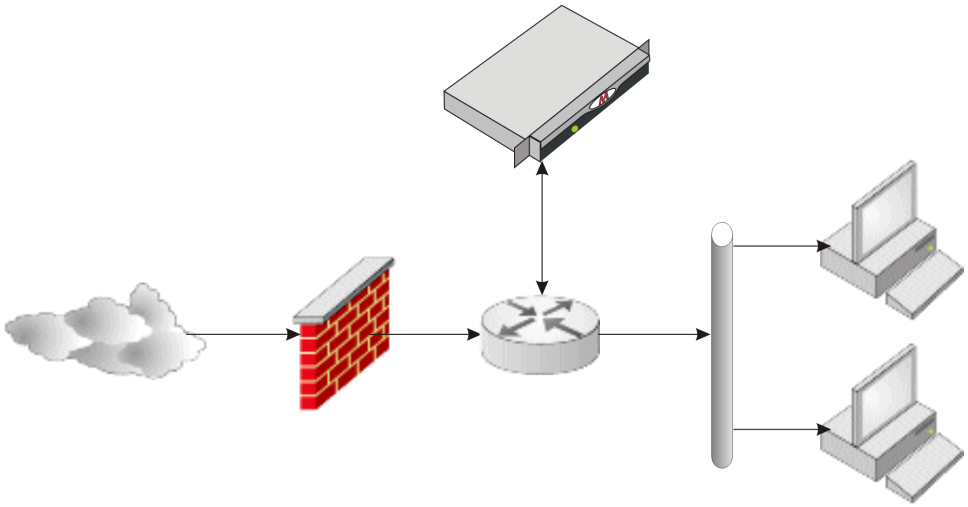


Abbildung 6: Konfiguration als expliziter Proxy

Das Gerät muss innerhalb Ihres Unternehmens hinter einer Firewall positioniert werden, wie in Abbildung 6: Konfiguration als expliziter Proxy dargestellt.

Normalerweise ist die Firewall so konfiguriert, dass der Datenverkehr, der nicht direkt von dem Gerät stammt, gesperrt wird.

Wenn Sie in Bezug auf die Topologie Ihres Netzwerks unsicher sind und nicht wissen, wie Sie das Gerät integrieren sollen, wenden Sie sich an Ihren Netzwerkspezialisten.

Verwenden Sie diese Konfiguration in folgenden Fällen:

- Das Gerät wird im Modus "Expliziter Proxy" betrieben.
- Sie verwenden E-Mail (SMTP).

Für diese Konfiguration gilt:

- Konfigurieren Sie die externen DNS-Server (Domain Name System) oder NAT (Network Address Translation) auf der Firewall so, dass der externe Mail-Server E-Mails an das Gerät zustellt, nicht an den internen Mail-Server.
- Konfigurieren Sie die internen Mail-Server so, dass E-Mail-Verkehr an das Gerät gesendet wird. Das heißt, die internen Mail-Server müssen das Gerät als Smart-Host verwenden. Vergewissern Sie sich, dass die Client-Geräte E-Mails an die E-Mail-Server in Ihrem Unternehmen senden können.
- Stellen Sie sicher, dass die Firewall-Regeln aktualisiert werden. Die Firewall muss den Datenverkehr von dem Gerät akzeptieren, darf aber keinen Datenverkehr verarbeiten, der direkt von den Client-Geräten kommt. Richten Sie Regeln ein, die verhindern, dass unerwünschter Datenverkehr in Ihr Unternehmen gelangt.

Ausbringungsstrategien für die Verwendung des Geräts in einer DMZ

Eine "demilitarisierte Zone" (Demilitarized Zone, DMZ) ist ein Netzwerk, das durch eine Firewall von allen anderen Netzwerken getrennt ist, auch vom Internet und anderen internen Netzwerken. Eine DMZ wird üblicherweise mit dem Ziel implementiert, den Zugriff auf Server zu sperren, die Internetdienste (beispielsweise E-Mail) zur Verfügung stellen.

Hacker verschaffen sich oft Zugriff auf Netzwerke, indem sie herausfinden, auf welchen TCP-/UDP-Ports Appliances Anfragen erwarten, und dann bekannte Schwachstellen in Appliances ausnutzen. Firewalls senken das Risiko solcher Exploits erheblich, indem sie den Zugriff auf bestimmte Ports auf bestimmten Servern steuern.

Das Gerät kann einfach zu einer DMZ-Konfiguration hinzugefügt werden. Die Art, wie Sie das Gerät in einer DMZ verwenden, hängt von den zu scannenden Protokollen ab.

Inhalt

- Vorbereitung der Installation
- SMTP-Konfiguration in einer DMZ

SMTP-Konfiguration in einer DMZ

Die DMZ ist eine gute Möglichkeit für das Verschlüsseln von E-Mails. Wenn der E-Mail-Verkehr die Firewall zum zweiten Mal erreicht (auf seinem Weg von der DMZ zum internen Netzwerk), ist er verschlüsselt.

Geräte, die SMTP-Verkehr in einer DMZ scannen können, sind normalerweise im Modus "Expliziter Proxy" konfiguriert.

Konfigurationsänderungen müssen nur an den MX-Einträgen für die E-Mail-Server vorgenommen werden.

HINWEIS: Sie können den Modus "Transparente Bridge" verwenden, wenn Sie SMTP in einer DMZ scannen. Wenn Sie jedoch den Datenfluss nicht richtig steuern, scannt das Gerät jede Nachricht zweimal, einmal in jede Richtung. Aus diesem Grund wird für SMTP-Scans normalerweise der Modus "Expliziter Proxy" verwendet.

E-Mail-Relay

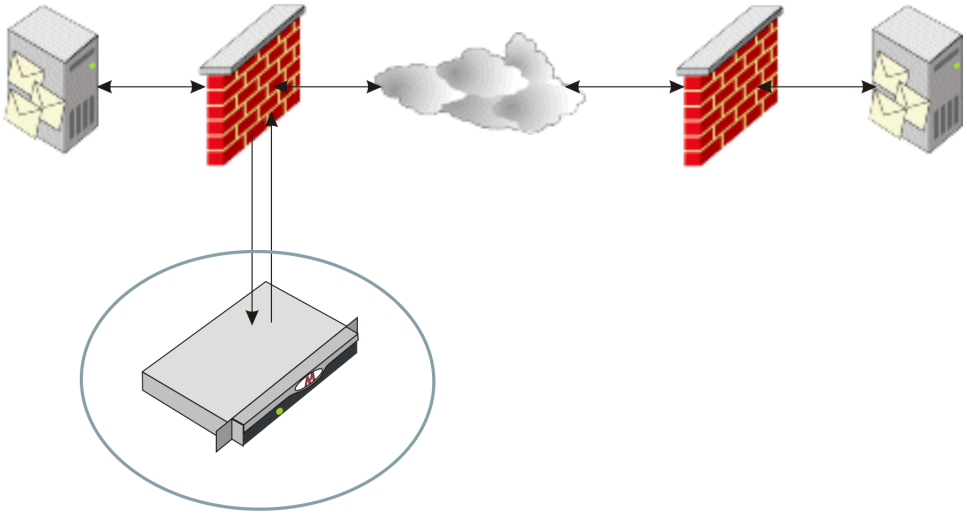


Abbildung 7: Konfiguration eines Geräts im Modus "Expliziter Proxy" in einer DMZ

Wenn Sie in Ihrer DMZ bereits ein Relay eingerichtet haben, können Sie es durch das Gerät ersetzen.

Um Ihre bestehenden Firewall-Richtlinien zu verwenden, geben Sie dem Gerät dieselbe IP-Adresse wie dem Mail-Relay.

E-Mail-Gateway

SMTP bietet keine Methoden zur Verschlüsselung von E-Mail-Nachrichten. Sie können mithilfe von TLS (Transport Layer Security) den Link verschlüsseln, nicht jedoch die E-Mail-Nachrichten. Daher erlauben einige Unternehmen solchen Datenverkehr nicht in ihrem internen Netzwerk. Zur Umgehung dieses Problems wird häufig ein proprietäres E-Mail-Gateway eingesetzt, zum Beispiel Lotus Notes® oder Microsoft® Exchange, um den E-Mail-Datenverkehr zu verschlüsseln, bevor er das interne Netzwerk erreicht.

Um eine DMZ-Konfiguration unter Verwendung des proprietären E-Mail-Gateways zu implementieren, fügen Sie das Scan-Gerät zur DMZ auf der SMTP-Seite des Gateways hinzu.

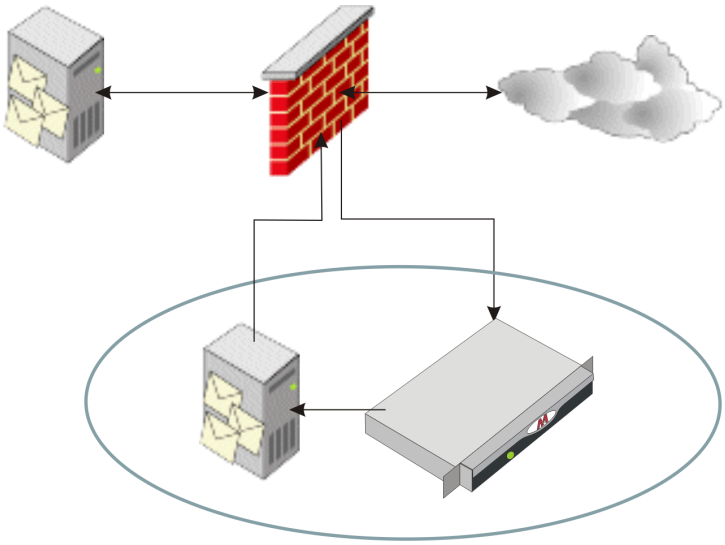


Abbildung 8: Schützen eines E-Mail-Gateways in einer DMZ

Nehmen Sie hierfür folgende Konfigurationen vor:

- Die öffentlichen MX-Einträge müssen externe Mail-Server anweisen, alle eingehenden E-Mail-Nachrichten an das Gerät (statt an das Gateway) zu senden.
- Das Gerät muss alle eingehenden E-Mail-Nachrichten an das Mail-Gateway und alle ausgehenden Nachrichten per DNS oder über ein externes Relay senden.
- Das E-Mail-Gateway muss alle eingehenden E-Mails an die internen Mail-Server und aller andere (ausgehenden) Mails an das Gerät weiterleiten.
- Die Firewall erlaubt nur eingehende E-Mails, die sich an das Gerät richten.

HINWEIS: Bei Firewalls, auf denen die Verwendung von NAT (Network Address Translation) konfiguriert ist und die eingehende E-Mails an die internen E-Mail-Server umleiten, müssen die öffentlichen MX-Einträge nicht neu konfiguriert werden. Sie leiten den Datenverkehr bereits an die Firewall und nicht an das eigentliche E-Mail-Gateway. In diesem Fall muss die Firewall neu konfiguriert werden, sodass eingehende Nachrichten an das Gerät geleitet werden.

Für Lotus Notes spezifische Firewall-Regeln

Lotus Notes-Server kommunizieren standardmäßig über TCP-Port 1352. Die für den Schutz von Notes-Servern in einer DMZ verwendeten Firewall-Regeln erlauben üblicherweise folgendem Datenverkehr das Passieren durch die Firewall:

- Eingehende SMTP-Anforderungen (TCP-Port 25) vom Internet, die für das Gerät bestimmt sind

- Anforderungen auf TCP-Port 1352 aus dem Notes-Gateway, die an einen internen Notes-Server gerichtet sind
- Anforderungen auf TCP-Port 1352 von einem internen Notes-Server, die an das Notes-Gateway gerichtet sind
- SMTP-Anforderungen vom Gerät, die für das Internet bestimmt sind

Alle anderen SMTP-Anforderungen und Anforderungen auf TCP-Port 1352 werden verweigert.

Für Microsoft Exchange spezifische Firewall-Regeln

Ein auf Microsoft Exchange basierendes E-Mail-System erfordert eine erhebliche Umkonfiguration.

Wenn Exchange-Server miteinander kommunizieren, senden sie die ersten Pakete mithilfe des RPC-Protokolls (TCP-Port 135). Sobald die ursprüngliche Kommunikation jedoch eingerichtet ist, werden zwei Ports dynamisch ausgewählt und verwendet, um alle nachfolgenden Pakete für den Rest der Kommunikation zu senden. Sie können die Firewall nicht so konfigurieren, dass sie diese dynamisch gewählten Ports erkennt. Deshalb leitet die Firewall diese Pakete nicht weiter.

Die Ausweichlösung lautet, die Registrierung auf jedem Exchange-Server zu modifizieren, der über die Firewall kommuniziert, sodass immer dieselben zwei "dynamischen" Ports verwendet werden, und dann TCP 135 und diese beiden Ports auf der Firewall zu öffnen.

Wir erwähnen diese Ausweichlösung, um eine umfassende Erklärung zu bieten, wir empfehlen sie jedoch nicht. Das RPC-Protokoll ist in Microsoft-Netzwerken weit verbreitet. Das Öffnen von TCP 135 für eingehenden Datenverkehr ist für die meisten Sicherheitsexperten ein rotes Tuch.

Wenn Sie diese Ausweichlösung verwenden möchten, finden Sie Details in den folgenden KnowledgeBase-Artikeln auf der Microsoft-Website:

- Q155831
- Q176466

Arbeitslastverwaltung

Die Appliance verfügt über eine eigene interne Arbeitslastverwaltung, durch die die Scan-Last gleichmäßig auf alle für die Zusammenarbeit konfigurierten Appliances verteilt wird.

Sie müssen keinen separaten externen Lastenausgleicher bereitstellen.

▸ Vorbereitung der Installation

Anschließen und Konfigurieren der Appliance

McAfee empfiehlt, dass Sie bei der Montage der Appliance folgende Reihenfolge einhalten:

1. Entpacken Sie die Appliance, und vergewissern Sie sich, dass keine Teile fehlen (prüfen Sie dies anhand der Teileliste in der Packung).
2. Montieren Sie die Appliance im Rack.
3. Schließen Sie die Peripheriegeräte (Monitor, Tastatur) und die Stromversorgung an.
4. Schließen Sie die Appliance an das Netzwerk an, und beachten Sie dabei Ausbringungsszenarien und den gewünschten Netzwerkmodus.
5. Installieren Sie die Software auf der Appliance.
6. Nehmen Sie die grundlegende Konfiguration (Servername, IP-Adresse, Gateway usw.) auf der Konfigurationskonsole vor.
7. Rufen Sie die Verwaltungsoberfläche auf.
8. Führen Sie den Setup-Assistenten aus.
9. Leiten Sie den Test-Netzwerkverkehr durch die Appliance.
10. Testen Sie, ob der Netzwerkverkehr gescannt wird.
11. Konfigurieren Sie Richtlinien und Berichte.
12. Leiten Sie den Produktionsverkehr durch die Appliance.

VORSICHT: Wenn Sie die Appliance an Ihr Netzwerk anschließen, können der Internetzugang oder andere Netzwerkdienste unterbrochen werden. Planen Sie einen Zeitraum ein, in dem das Netzwerk nicht verfügbar ist, vorzugsweise zu einer Zeit mit geringer Netzwerkauslastung.

Inhalt

- Kurzanleitungstabelle für die Installation
- Montieren der Appliance
- Verbindung mit dem Netzwerk
- Anschließen der Appliance an das Stromnetz
- Verwenden der Konfigurationskonsole

Kurzanleitungstabelle für die Installation

Führen Sie die in der folgenden Tabelle aufgeführten Schritte aus, um die Appliance zu installieren:

Schritt		Beschreibung
1.	Packen Sie alle Komponenten aus, und prüfen Sie den Inhalt anhand der Teilelisten in der Kiste.	Lieferumfang

Schritt		Beschreibung
2.	Schließen Sie die Peripheriegeräte und die Stromversorgung an.	Monitor und Tastatur
3.	Schließen Sie die Appliance an das Netzwerk an.	Verbindung mit dem Netzwerk
4.	Installieren Sie die Software.	Installieren der Software
5.	Führen Sie die grundlegende Konfiguration durch.	Verwenden der Konfigurationskonsole
6.	Rufen Sie die Verwaltungsoberfläche auf.	Verwenden der Konfigurationskonsole
7.	Leiten Sie den Testnetzwerkverkehr durch die Appliance.	Testen des Geräts
8.	Testen Sie, ob der Netzwerkverkehr gescannt wird.	Testen des Geräts
9.	Konfigurieren Sie Richtlinien und Berichte.	Verwenden von Richtlinien für die Verwaltung von Nachrichten-Scans
10.	Konfigurieren Sie den Produktionsverkehr durch das System.	Verwenden der Konfigurationskonsole

Anschlüsse und Verbindungen

Weitere Informationen über die Anschlüsse Ihrer Appliance finden Sie in der *Beschreibung der Hardware-Anschlüsse für McAfee Email and Web Security 2010 Appliances*.

Montieren der Appliance

Gehen Sie wie nachfolgend beschrieben vor, um die Appliance zu montieren.

Vorgehensweise

1. Nehmen Sie die Appliance aus der Schutzverpackung, und legen Sie sie auf eine ebene Fläche.
2. Wenn Sie die Appliance in einem 19-Zoll-Rack installieren, führen Sie die Schritte unter Montieren der Appliance in einem Rack aus.
3. Schließen Sie einen Monitor, eine Tastatur und eine Maus an die Appliance an.
4. Verbinden Sie die Netzkabel mit dem Monitor und der Appliance, schließen Sie sie jedoch noch nicht an die Spannungsversorgung an.
5. Schließen Sie die Appliance unter Beachtung des gewählten Betriebsmodus an das Netzwerk an.

Montieren der Appliance in einem Rack

Das Montage-Set ermöglicht die Installation in einem zweireihigen Rack. Das Montage-Set kann für die meisten 19-Zoll-Racks nach Industriestandard verwendet werden.

Das Montage-Set beinhaltet:

- 2 Halteschienen
- 8 Schrauben
- 2 wiederverwendbare Kabelbinder

Sie benötigen einen für die Schrauben passenden Schraubendreher.

VORSICHT:

Beachten Sie unbedingt die Sicherheitswarnungen. Beladen Sie das Rack immer von unten nach oben. Wenn Sie mehrere Appliances installieren, sollten Sie mit der untersten freien Stelle beginnen.

Verbindung mit dem Netzwerk

In diesem Abschnitt wird erläutert, wie die Appliance an Ihr Netzwerk angeschlossen wird.

Welche Anschlüsse und Kabel Sie dazu verwenden, hängt vom Betriebsmodus der Appliance ab. Informationen zu Netzwerkmodi finden Sie unter Überlegungen zu Netzwerkmodi.

Port-Nummern

Verwenden Sie die folgenden Port-Nummern, wenn Sie die Appliance mit Ihrem Netzwerk verbinden.

- Verwenden Sie Port 443 für HTTPS.
- Verwenden Sie Port 80 für HTTP.
- Verwenden Sie Port 25 für SMTP.
- Verwenden Sie Port 110 für POP3.
- Verwenden Sie Port 21 für FTP.

Verwenden von Kupfer-LAN-Verbindungen

Verwenden Sie die LAN1- und LAN2-Switch-Verbindungen und die im Lieferumfang enthaltenen Netzwerkkabel (oder entsprechende Cat-5e- bzw. Cat-6-Ethernet-Kabel), und schließen Sie die Appliance entsprechend dem gewählten Netzwerkmodus an Ihr Netzwerk an.

Falls Sie in Ihrem Netzwerk DHCP konfiguriert haben, werden die IP-Adressen für diese Anschlüsse jetzt automatisch zugewiesen.

Modus "Transparente Bridge"

Schließen Sie die LAN1- und LAN2-Switches der Appliance mit den mitgelieferten Kupfer-LAN-Kabeln an Ihr Netzwerk an, um die Appliance in den Datenstrom einzufügen.

Modus "Transparenter Router"

Die Appliance fungiert als Router. Die LAN-Segmente, die mit ihren beiden Netzwerkschnittstellen verbunden sind, müssen sich deshalb in verschiedenen IP-Subnetzen befinden. Sie muss einen bestehenden Router ersetzen, oder auf der Seite der Appliance muss ein neues Subnetz angelegt werden. Ändern Sie hierfür die IP-Adresse oder die Netzmaske, die die Computer auf dieser Seite verwenden.

Modus "Expliziter Proxy"

Schließen Sie den LAN1- oder LAN2-Switch mit einem Kupfer-LAN-Kabel (mitgeliefert) an das Netzwerk an. Bei diesem Kabel handelt es sich um ein durchgängiges (ungekreuztes) Kabel, das die Appliance mit einem normalen, ungekreuzten RJ-45-Netzwerk-Switch verbindet.

Im Modus "Expliziter Proxy" kann die nicht verwendete Switch-Verbindung als dedizierter Management-Port verwendet werden. Um die Appliance lokal verwalten zu können, schließen Sie die Appliance über ein gekreuztes Cat-5e-Ethernet-Kabel an die Netzwerkkarte des lokalen Computers an.

Verwenden von Glasfaser-LAN-Verbindungen

Schließen Sie die LAN1- und LAN2-Konnektoren mit Glasfaserkabeln an das Netzwerk an. Welche Konnektoren Sie verwenden, hängt vom Betriebsmodus der Appliance ab.

Modus "Transparente Bridge"

Schließen Sie die LAN1- und LAN2-Switches mit Glasfaserkabeln an das Netzwerk an.

Modus "Transparenter Router"

Schließen Sie die LAN1- und LAN2-Switches mit Glasfaserkabeln an verschiedene IP-Subnetze an.

Modus "Expliziter Proxy"

Schließen Sie den LAN1-Switch der Appliance mit einem Glasfaserkabel an das Netzwerk an.

Im Modus "Expliziter Proxy" kann der nicht verwendete Konnektor als dedizierter Management-Port verwendet werden. Wenn der Verwaltungscomputer über eine kompatible Netzwerkkarte verfügt, schließen Sie ihn zur lokalen Verwaltung an den verbleibenden Konnektor an.

Monitor und Tastatur

Schließen Sie einen Monitor und eine Tastatur an die Appliance an.

Anschließen der Appliance an das Stromnetz

Gehen Sie wie nachfolgend beschrieben vor, um die Appliance an das Stromnetz anzuschließen und einzuschalten.

Vorgehensweise

1. Schließen Sie die Netzkabel der Appliance und des Monitors an die Stromsteckdosen an.

   HINWEIS: Falls das Netzkabel für das Einsatzland nicht geeignet ist, setzen Sie sich mit Ihrem Händler in Verbindung.

2. Schalten Sie die Appliance ein, indem Sie den Netzschalter drücken. Nach dem Hochfahren wird die Konfigurationskonsole auf dem Monitor angezeigt. Siehe Verwenden der Konfigurationskonsole.

Installieren der Software

Gehen Sie folgendermaßen vor, um die Email and Web Security Software auf dem Gerät zu installieren.

Vorgehensweise

1. Laden Sie von einem Computer mit Internetzugang aus die neueste Version der Email and Web Security Software von der McAfee-Download-Seite herunter. (Sie benötigen hierfür Ihre Grant-Nummer.)
2. Erstellen Sie von diesem Image eine CD.
3. Schließen Sie einen Monitor, eine Tastatur und eine Maus an das Gerät an.
4. Schalten Sie das Gerät ein, und legen Sie die CD in das CD-ROM-Laufwerk ein.
5. Starten Sie das Gerät neu. Die Software wird auf dem Gerät installiert.

Verwenden der Konfigurationskonsole

Mit der Software der Version 5.5 wurde der Konfigurationsprozess vereinfacht. Sie können Ihr Gerät jetzt entweder von der Konfigurationskonsole aus oder innerhalb der Benutzeroberfläche mit dem Setup-Assistenten konfigurieren.

Die Konfigurationskonsole wird am Ende der Startsequenz automatisch gestartet, entweder nachdem:

- ein unkonfiguriertes Gerät gestartet wurde
- oder nachdem ein Gerät auf seine Werkseinstellungen zurückgesetzt wurde.

Wird die Konfigurationskonsole gestartet, bietet Sie Ihnen die Möglichkeit, Ihr Gerät von der Gerätekonsole aus in Ihrer bevorzugten Sprache zu konfigurieren, bzw. liefert Anweisungen dafür, wie Sie von einem anderen Computer im selben Klasse-C-Subnetz aus eine Verbindung mit dem Setup-Assistenten innerhalb der Benutzeroberfläche herstellen können. Beide Methoden bieten Ihnen dieselben Optionen für die Konfiguration Ihres Geräts.

HINWEIS: Von der Konfigurationskonsole aus können Sie eine neue Installation der Appliance-Software konfigurieren. Wenn Sie jedoch für die Konfiguration Ihrer Appliance eine zuvor gespeicherte Konfigurationsdatei verwenden möchten, müssen Sie sich bei der Benutzeroberfläche der Appliance anmelden und den Setup-Assistenten ausführen (**System | Setup-Assistent**).

Ebenso wird mit dieser Softwareversion für folgende Parameter die automatische Konfiguration mithilfe von DHCP eingeführt:

- Host-Name
- Domänenname
- Standard-Gateway
- DNS-Server
- Geleaste IP-Adresse
- NTP-Server

▸ Begrüßungsseite
▸ Durchführen einer Standardinstallation
▸ Durchführen der benutzerdefinierten Einrichtung

▸ Wiederherstellung aus einer Datei
▸ Einrichten der Verwaltung durch ePO

Begrüßungsseite

Dies ist die erste Seite des Setup-Assistenten. Auf dieser Seite können Sie den gewünschten Installationstyp auswählen.

HINWEIS: Wenn Sie über den Setup-Assistenten auf diese Seite zugreifen, werden Sie zur Eingabe Ihres Benutzernamens und Kennworts aufgefordert.

- Wählen Sie **Standardeinrichtung** (Standardeinstellung), um das Gerät im Modus "Transparente Bridge" einzurichten und für den Schutz Ihres Netzwerks zu konfigurieren. Konfigurieren Sie das Gerät nur für den Modus "Transparente Bridge". Wenn Sie wählen, dass E-Mail-Verkehr geschützt werden soll, wird das SMTP-Protokoll aktiviert. Wenn Sie wählen, dass Web-Verkehr geschützt werden soll, wird das HTTP-Protokoll aktiviert.
- Wählen Sie **Benutzerdefinierte Einrichtung**, um den Betriebsmodus für Ihr Gerät auszuwählen. Wenn Sie auswählen, dass E-Mail-Verkehr geschützt werden soll, können SMTP und POP3 aktiviert werden. Wenn Sie auswählen, dass Web-Verkehr geschützt werden soll, können HTTP, FTP und ICAP aktiviert werden. Verwenden Sie diese Art der Einrichtung, um IPv6 zu konfigurieren und sonstige Änderungen an der Standardkonfiguration vorzunehmen.
- Wählen Sie **Wiederherstellen aus Datei** (auf der Konfigurationskonsole nicht verfügbar), um Ihr Gerät basierend auf einer zuvor gespeicherten Konfiguration einzurichten. Nach dem Importieren der Datei können Sie die importierten Einstellungen überprüfen, bevor Sie den Assistenten abschließen.
- Wählen Sie **Einrichten der Verwaltung durch ePO** (nur Email and Web Security Appliances v5.6), um Ihr Gerät so einzurichten, dass es vom ePolicy Orchestrator-Server verwaltet werden kann. Es wird nur ein Minimum an Informationen benötigt, da das Gerät die meisten Konfigurationsdaten vom ePolicy Orchestrator-Server enthält.

Durchführen einer Standardinstallation

Bei der **Standardeinrichtung** enthält der Assistent die folgenden Seiten:

- **Datenverkehr**
- **Grundlegende Einstellungen**
- **Zusammenfassung**

HINWEIS: Mit der Wahl der Standardeinrichtung wird für das Gerät der Modus "Transparente Bridge" erzwungen.

Datenverkehr

Über diese Seite können Sie den Typ von Datenverkehr angeben, den das Gerät scannt.

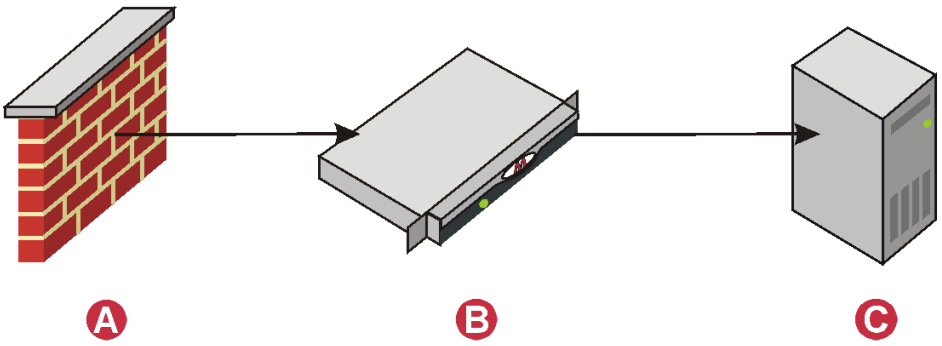
Optionsbeschreibungen

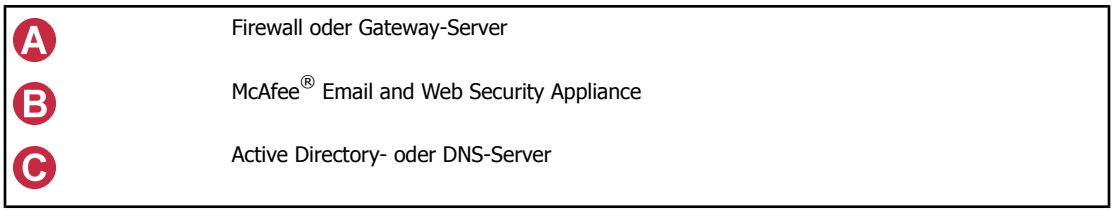
Option	Beschreibung
Web-Verkehr scannen	Web-Verkehr umfasst nur HTTP-Verkehr. Nach der Installation:

Option	Beschreibung
	• Das Gerät schützt Ihr Netzwerk vor Viren und verwendet McAfee SiteAdvisor beim Besuch von Websites. • Wenn Sie mehrere Arten von Datenverkehr scannen möchten, können Sie die einzelnen Protokolle über die jeweilige Seite aktivieren. Wählen Sie aus dem Menü **Web | Web-Konfiguration | HTTP**, **Web | Web-Konfiguration | ICAP** oder **Web | Web-Konfiguration | FTP**. Außerdem können Sie Folgendes auswählen: • **Schutz gegen potentiell unerwünschte Programme (einschließlich Spyware) aktivieren** McAfee Anti-Spyware schützt Ihr Netzwerk vor vielen Arten potenziell unerwünschter Software, wie Spyware, Adware, Remote-Verwaltungs-Tools, Dialern und Kennwort-Crackern. Diese Funktion ist standardmäßig nicht aktiviert. HINWEIS: McAfee Anti-Spyware wurde dazu entwickelt, potenziell unerwünschte Programme (PUPe) zu erkennen und mit Ihrer Erlaubnis zu entfernen. Manche gekauften oder absichtlich heruntergeladenen Programme agieren als Hosts für potenziell unerwünschte Programme. Wenn diese potenziell unerwünschten Programme entfernt werden, funktionieren ihre Hosts möglicherweise nicht mehr. Genaue Informationen entnehmen Sie bitte dem Lizenzvertrag für das jeweilige Hostprogramm. McAfee, Inc. fordert weder zum Bruch von abgeschlossenen Lizenzverträgen auf, noch duldet es dies. Lesen Sie Lizenzverträge und Datenschutzrichtlinien unbedingt gründlich durch, bevor Sie Software herunterladen oder installieren.
E-Mail-Verkehr scannen	E-Mail-Verkehr umfasst nur SMTP-Verkehr. Nach der Installation: • Das Gerät schützt Ihr Netzwerk vor Viren, Spam und Phishing und verwendet McAfee TrustedSource, um Ihr Netzwerk vor unerwünschten E-Mails zu schützen. • Wenn Sie mehrere Arten von Datenverkehr scannen möchten, können Sie die einzelnen Protokolle über die jeweilige Seite aktivieren. Wählen Sie aus dem Menü **E-Mail | E-Mail-Konfiguration | Protokollkonfiguration | Verbindungseinstellungen (POP3)** oder **E-Mail | E-Mail-Konfiguration | Protokollkonfiguration | Verbindungseinstellungen (SMTP)**. Außerdem können Sie Folgendes auswählen: • **Schutz gegen potentiell unerwünschte Programme (einschließlich Spyware) aktivieren**
Lokale Relay-Domäne	Unter **Relay-Optionen** schlägt das Gerät die Domäneninformationen vor, sofern diese über DHCP verfügbar sind. Löschen Sie den Stern, wenn Sie den vorgeschlagenen Domänennamen verwenden möchten, oder geben Sie einen anderen Domänennamen ein.

Grundlegende Einstellungen

Verwenden Sie diese Seite, um grundlegende Einstellungen für die Appliance im Modus "Transparente Bridge" anzugeben.





HINWEIS: Einige dieser Einstellungen werden automatisch von Ihrem Netzwerk-DHCP-Server aus konfiguriert.

Optionsbeschreibungen

Option	Beschreibung
Gerätename	Gibt einen Namen an, zum Beispiel "Gerät1".
Domänenname	Gibt einen Domänennamen an, z. B. domaene1.com.
IP-Adresse	Gibt eine IP-Adresse an, z. B. 198.168.200.10. Der vollqualifizierte Domänenname (**Gerätename**. **Domänenname**) muss in diese IP-Adresse aufgelöst werden, wenn der DNS-Server (hier angegeben) aufgerufen wird. McAfee empfiehlt, dass diese IP-Adresse bei einer umgekehrten Suche in den vollqualifizierten Domänennamen aufgelöst wird.
Subnetz	Gibt eine Subnetzadresse an, z. B. 255.255.255.0.
Gateway-IP	Gibt eine IP-Adresse an, z. B. 198.168.10.1. Hierbei handelt es sich meist um einen Router oder eine Firewall. Sie können später testen, ob die Appliance mit diesem Gerät kommunizieren kann.
DNS-Server-IP	Gibt die Adresse eines Domänennamenservers an, den die Appliance verwendet, um Website-Adressen in IP-Adressen umzuwandeln. Dabei kann es sich um einen Active Directory- oder einen DNS-Server handeln. Sie können später testen, ob die Appliance mit diesem Server kommunizieren kann.
Modus	Gibt den Modus an – Transparente Bridge.
Benutzer-ID	Beim Benutzer "scmadmin" handelt es sich um den Superadministrator. Dieses Konto kann weder geändert oder deaktiviert noch gelöscht werden. Nach der Installation können Sie jedoch weitere Anmeldekonten hinzufügen.
Kennwort	Gibt das neue Kennwort an. Ändern Sie das Kennwort baldmöglichst, damit Ihre Appliance geschützt bleibt. Sie müssen das neue Kennwort zweimal eingeben, um es zu bestätigen. Das ursprüngliche Standardkennwort lautet **scmchangeme**.
Zeitzone	Bietet eine Auswahl an Zeitzonen. Die Zonen sind von West nach Ost organisiert und decken den pazifischen Raum, Amerika, Europa, Asien, Afrika, Indien, Japan und Australien ab.
Systemzeit	Gibt das Datum und die lokale Uhrzeit an. Klicken Sie auf das Kalendersymbol, um das Datum festzulegen.
Uhrzeit jetzt einstellen	Wenn Sie darauf klicken, wird die Zeit in der Appliance eingestellt. Sie müssen auf diese Schaltfläche klicken, bevor Sie auf **Weiter** klicken. Falls erforderlich, können Sie nach der Installation NTP (Network Time Protocol) konfigurieren.

Zusammenfassung

Auf dieser Seite können Sie eine Zusammenfassung der Einstellungen anzeigen, die Sie im Setup-Assistenten vorgenommen haben. Wenn Sie einen Wert ändern möchten, klicken Sie auf den entsprechenden blauen Link, um die Seite anzuzeigen, auf der Sie den Wert ursprünglich eingegeben haben.

Nachdem Sie auf **Fertig stellen** geklickt haben, wird der Setup-Assistent abgeschlossen.

Verwenden Sie die auf dieser Seite angezeigte IP-Adresse, um die Benutzeroberfläche aufzurufen. Beispiel: https://192.168.200.10. Beachten Sie, dass die Adresse mit https und nicht mit http beginnt.

Wenn Sie sich zum ersten Mal bei der Benutzeroberfläche anmelden, geben Sie den Benutzernamen **scmadmin** und das Kennwort ein, das Sie in diesem Setup-Assistenten angegeben haben.

Optionsbeschreibungen

Option	Beschreibung
	Der Wert entspricht bewährten Praktiken.
	Der Wert ist wahrscheinlich nicht korrekt. Er ist zwar gültig, entspricht aber nicht bewährten Praktiken. Prüfen Sie den Wert, bevor Sie fortfahren.
	Es wurde kein Wert festgelegt. Der vorgegebene Standardwert wurde nicht geändert. Prüfen Sie den Wert, bevor Sie fortfahren.

▸ Einrichten der Verwaltung durch ePO

Durchführen der benutzerdefinierten Einrichtung

Bei der benutzerdefinierten Einrichtung enthält der Assistent die folgenden Seiten:

- Datenverkehr
- Grundlegende Einstellungen
- Netzwerkeinstellungen
- Cluster-Verwaltung
- DNS und Routing
- Zeiteinstellungen
- Kennwort
- Zusammenfassung

Datenverkehr

Über diese Seite können Sie den Typ von Datenverkehr angeben, den das Gerät scannt.

- Web-Verkehr umfasst HTTP (für Web-Browsing), ICAP (zur Verwendung mit ICAP-Clients) und FTP für die Dateiübertragung.
- Der E-Mail-Verkehr umfasst SMTP und POP3.

Sie können die einzelnen Protokolle (SMTP, POP3, HTTP, ICAP und FTP) aktivieren oder deaktivieren. Wenn sich das Gerät im Modus "Transparenter Router" oder "Transparente Bridge" befindet und ein Protokoll deaktiviert wird, passiert der Datenverkehr des jeweiligen Protokolls das Gerät, wird aber nicht gescannt.

Wenn sich das Gerät im Modus "Expliziter Proxy" befindet und ein Protokoll deaktiviert wird, wird der Verkehr abgelehnt, der für dieses Protokoll an den Blade-Server gesendet wird. Das Protokoll wird im Gerät blockiert. Im Modus "Expliziter Proxy" wird nur SMTP-, POP3-, HTTP-,

ICAP- und FTP-Verkehr vom Blade-Server verarbeitet. Sämtlicher anderer Datenverkehr wird abgelehnt.

Wenn nach der Installation gar kein Datenverkehr gescannt werden soll, können Sie alle Protokolle auf dieser Seite deaktivieren. Wählen Sie im Menü **E-Mail | E-Mail-Konfiguration | Protokollkonfiguration** oder **Web | Web-Konfiguration**.

Optionsbeschreibungen

Option	Beschreibung
Web-Verkehr scannen	Web-Verkehr umfasst HTTP-, FTP- und ICAP-Verkehr. Nach der Installation: Das Gerät schützt Ihr Netzwerk vor Viren und verwendet McAfee SiteAdvisor beim Besuch von Websites. Des Weiteren stehen die folgenden Optionen zur Verfügung: • **Schutz gegen potentiell unerwünschte Programme (einschließlich Spyware) aktivieren** McAfee Anti-Spyware schützt Ihr Netzwerk vor vielen Arten potenziell unerwünschter Software, wie Spyware, Adware, Remote-Verwaltungs-Tools, Dialern und Kennwort-Crackern. Diese Funktion ist standardmäßig nicht aktiviert. HINWEIS: McAfee Anti-Spyware wurde dazu entwickelt, potenziell unerwünschte Programme (PUPe) zu erkennen und mit Ihrer Erlaubnis zu entfernen. Manche gekauften oder absichtlich heruntergeladenen Programme agieren als Hosts für potenziell unerwünschte Programme. Wenn diese potenziell unerwünschten Programme entfernt werden, funktionieren ihre Hosts möglicherweise nicht mehr. Genaue Informationen entnehmen Sie bitte dem Lizenzvertrag für das jeweilige Hostprogramm. McAfee, Inc. fordert weder zum Bruch von abgeschlossenen Lizenzverträgen auf, noch duldet es dies. Lesen Sie Lizenzverträge und Datenschutzrichtlinien unbedingt gründlich durch, bevor Sie Software herunterladen oder installieren. • **HTTP-Verkehr scannen** • **ICAP-Server aktivieren** • **FTP-Verkehr scannen**
E-Mail-Verkehr scannen	Der E-Mail-Verkehr umfasst SMTP- und POP3-Verkehr. Nach der Installation: Das Gerät schützt Ihr Netzwerk vor Viren, Spam und Phishing und verwendet McAfee TrustedSource, um Ihr Netzwerk vor unerwünschten E-Mails zu schützen. Des Weiteren stehen die folgenden Optionen zur Verfügung: • **Schutz gegen potentiell unerwünschte Programme (einschließlich Spyware) aktivieren** • **SMTP-Verkehr scannen** • **POP3-Verkehr scannen**
Lokale Relay-Domäne	Unter **Relay-Optionen** schlägt das Gerät die Domäneninformationen vor, sofern diese über DHCP verfügbar sind. Löschen Sie den Stern, wenn Sie den vorgeschlagenen Domänennamen verwenden möchten, oder geben Sie einen anderen Domänennamen ein.

Grundlegende Einstellungen

Verwenden Sie diese Seite, um grundlegende Einstellungen für das Gerät anzugeben.

Das Gerät zeigt einige Informationen an, die gelb markiert sind. Um diese Informationen zu ändern, klicken Sie, und geben Sie sie erneut ein.

Optionsbeschreibungen

Option	Beschreibung
Cluster-Modus	• **Aus** – Dies ist eine Standard-Appliance. • **Cluster-Scanner** – Die Appliance empfängt ihre Scan-Arbeit von einer Master-Appliance. • **Cluster-Master** – Die Appliance steuert die Scan-Arbeit verschiedener anderer Appliances. • **Cluster-Failover** – Falls der Master ausfällt, steuert stattdessen diese Appliance die Scan-Arbeit.
Gerätename	Gibt einen Namen an, z. B. Appliance1.
Domänenname	Gibt einen Namen an, z. B. domäne.beispiel.com.
Standard-Gateway (IPv4)	Gibt eine IPv4-Adresse an, z. B. 198.168.10.1. Sie können später testen, ob die Appliance mit diesem Server kommunizieren kann.
Nächster Hop-Router (IPv6)	Gibt eine IPv6-Adresse an, z. B. FD4A:A1B2:C3D4::1.

▸ Einrichten der Verwaltung durch ePO

Netzwerkeinstellungen

Wenn Sie für eine neue Installation zum ersten Mal eine Konfiguration ausführen (oder die Standardeinstellung wiederherstellen), wird die Seite "Netzwerkeinstellungen" angezeigt. Wenn Sie den Cluster-Modus des Geräts ändern, wird diese Seite ebenfalls angezeigt.

Verwenden Sie diese Seite, um die IP-Adresse, die Netzwerkgeschwindigkeiten und den Betriebsmodus für das Gerät zu konfigurieren.

Wenn möglich, füllt das Gerät viele dieser Optionen mithilfe von DHCP aus. Die IP-Adressen müssen eindeutig und für Ihr Netzwerk geeignet sein. Geben Sie nur so viele IP-Adressen wie erforderlich an.

Optionsbeschreibungen

Option	Beschreibung
Netzwerkeinstellungen ändern	Durch Klicken auf diese Option wird ein Assistent mit den folgenden Optionen gestartet.
Betriebsmodus	Bietet eine Auswahl an Modi. Im Modus **Transparenter Router** oder **Transparente Bridge** wissen andere Netzwerkgeräte wie beispielsweise E-Mail-Server nicht, dass der Blade-Server die E-Mail vor dem Weiterleiten abgefangen und gescannt hat. Der Vorgang ist für andere Geräte **transparent**. Im Modus **Expliziter Proxy** senden einige Netzwerkgeräte Datenverkehr an die Appliance. Der Blade-Server fungiert dann als **Proxy** und verarbeitet den Datenverkehr für die Geräte.
LAN-Schnittstellentyp	Gibt den Verbindungstyp an – Kupferleitung oder Glasfaser. Diese Option ist nur für High-Speed-Appliances verfügbar.
IP-Adresse	Gibt Netzwerkadressen an, die es der Appliance ermöglichen, mit Ihrem Netzwerk zu kommunizieren. Beispiel: 198.168.10.1 oder FD4A:A1B2:C3D4::1. Sie können mehrere IP-Adressen für die Anschlüsse der Appliance angeben. Wenn sich die Appliance im transparenten Modus befindet, werden die IP-Adressen für beide Anschlüsse in einer Liste zusammengefasst. Klicken Sie in den anderen Modi auf "Netzwerk-Schnittstelle 1" bzw. "Netzwerk-Schnittstelle 2", um die jeweilige Liste zu bearbeiten.

Option	Beschreibung
	Konfigurieren Sie die IP-Adresse für die Failover-Appliance. Wenn Sie im Modus "Expliziter Proxy" oder "Transparenter Router" arbeiten, erstellen Sie eine virtuelle IP-Adresse. Die virtuelle IP-Adresse muss für den Master- und den Failover-Management-Blade-Server gleich sein. Bei der ersten IP-Adresse in der Liste handelt es sich um die primäre Adresse. Bei den nachfolgenden IP-Adressen handelt es sich um Aliasadressen.
Netzwerkmaske	Gibt die IPv4-Netzwerkmaske an, z. B. 255.255.255.0, oder gibt die IPv6-Präfixlänge an (1-64 oder 128).

▸ Einrichten der Verwaltung durch ePO

Cluster-Verwaltung

Mithilfe dieser Seite können Sie die Anforderungen an den Lastenausgleich angeben.

- Konfiguration der Cluster-Verwaltung (Standard-Appliance)
- Cluster-Verwaltung (Cluster-Scanner)
- Cluster-Verwaltung (Cluster-Master)
- Cluster-Verwaltung (Cluster-Failover)

Ein *Cluster* ist eine Gruppe von Geräten, die gemeinsame Konfigurationen haben und den Netzwerkverkehr untereinander aufteilen.

Der Cluster kann Folgendes enthalten:

- Einen *Cluster-Master*. Der Master synchronisiert die Konfiguration und verteilt die Last des Netzwerkverkehrs auf die anderen Cluster-Mitglieder.

Weiterhin wird mindestens eines der folgenden Elemente benötigt:

- Ein *Cluster-Failover*. Falls der Cluster-Master ausfällt, übernimmt das Cluster-Failover nahtlos die Arbeit des Cluster-Masters.
- Einen oder mehrere *Cluster-Scanner*. Diese scannen den Datenverkehr gemäß den vom Master synchronisierten Richtlinien.

Beachten Sie, dass der Master und das Failover ebenfalls Datenverkehr scannen können.

Vorzüge

- Eine skalierbare Leistung aufgrund des Lastenausgleichs zwischen mehreren Geräten macht teure Upgrades überflüssig.
- Eine einfachere Verwaltung durch die Synchronisierung von Konfiguration und Aktualisierungen verringert den Verwaltungsaufwand.
- Eine verbesserte Stabilität durch hohe Verfügbarkeit vermindert das Risiko ungeplanter Ausfälle.
- Verbesserte Analyse durch konsolidierte Berichte.

Einrichten des Clusters

Alle Mitglieder des Clusters müssen separat installiert und konfiguriert werden.

Beim Konfigurieren eines Masters oder Failovers muss der Administrator Folgendes tun:

- Für den Proxy-Modus oder den Modus "Transparenter Router" eine virtuelle IP-Adresse festlegen, die für den Master und das Failover gleich ist. Die Cluster-Mitglieder verwenden dann für ein Failover VRRP.

- Für den Modus "Transparente Bridge" den Cluster zur Verwendung von STP im Fall eines Failovers einrichten. Die Bridge-Priorität muss auf dem Master niedriger sein (standardmäßig eingestellt).

Für alle Cluster-Mitglieder muss der Administrator die *Cluster-Kennung* festlegen. Diese eindeutige Kennung stellt sicher, dass die Mitglieder des Clusters korrekt miteinander verbunden werden. Zum Erstellen mehrerer Cluster können Sie für jeden Cluster eine unterschiedliche Kennung verwenden.

Leiten Sie den gesamten zu scannenden Netzwerkverkehr an den Cluster-Master (oder an die virtuelle IP-Adresse, wenn ein Cluster-Failover verwendet wird).

Verwalten des Clusters

Nachdem der Cluster konfiguriert wurde, wird er automatisch mithilfe der Cluster-Kennung verbunden. Das Dashboard des Cluster-Masters zeigt den Geräte- und den Cluster-Typ an.

Der Administrator muss Verwaltungsaufgaben, wie zum Beispiel das Festlegen von Scan-Richtlinien, anschließend nur in der Benutzeroberfläche des Cluster-Masters ausführen. Der Cluster-Master gibt dann diese Konfiguration automatisch an die anderen Cluster-Mitglieder weiter.

Der Cluster-Master fasst Folgendes zusammen:

- Antiviren-Aktualisierungen
- Berichte
- E-Mail in der Warteschlange
- McAfee Quarantine Manager (MQM)

HINWEIS: Software-Patches müssen nacheinander auf jedes einzelne Gerät übernommen werden.

Konfiguration der Cluster-Verwaltung (Standard-Appliance)

Die Cluster-Verwaltung ist deaktiviert.

Cluster-Verwaltung (Cluster-Scanner)

Verwenden Sie diese Seite, um Informationen für eine Scan-Appliance anzugeben.

Option	Beschreibung
Cluster-Kennung	Gibt eine ID an. Der Bereich liegt zwischen 0 und 65535.

Cluster-Verwaltung (Cluster-Master)

Verwenden Sie diese Seite, um Informationen für eine Master-Appliance anzugeben.

Option	Beschreibung
Für Lastenausgleich zu verwendende Adresse	Gibt die Appliance-Adresse an.
Cluster-Kennung	Gibt eine ID an. Der Bereich liegt zwischen 0 und 65535.
Scannen auf dieser Appliance aktivieren	Wenn diese Option nicht ausgewählt ist, verteilt diese Appliance die gesamte Scan-Arbeitslast auf die Scan-Appliances. HINWEIS: Bei Systemen mit zwei oder drei Appliances ist es sinnvoll, das Scannen auf allen Appliances aktivieren. Bei umfangreicheren Systemen empfiehlt es sich in der Regel, das Scannen nicht auf dem Cluster-Master zu aktivieren.

Cluster-Verwaltung (Cluster-Failover)

Verwenden Sie diese Seite, um Informationen für eine Failover-Appliance anzugeben.

Option	Beschreibung
Für Lastenausgleich zu verwendende Adresse	Gibt die Appliance-Adresse an. Bietet eine Liste aller einer Appliance zugewiesenen Subnetze.
Cluster-Kennung	Gibt eine ID an. Der Bereich liegt zwischen 0 und 65535.
Scannen auf dieser Appliance aktivieren	Wenn diese Option nicht ausgewählt ist, verteilt diese Appliance die gesamte Scan-Arbeitslast auf die Scan-Appliances. HINWEIS: Bei Systemen mit zwei oder drei Appliances ist es sinnvoll, das Scannen auf allen Appliances aktivieren. Bei umfangreicheren Systemen empfiehlt es sich in der Regel, das Scannen nicht auf dem Cluster-Failover zu aktivieren.

▸ Einrichten der Verwaltung durch ePO

DNS und Routing

Verwenden Sie diese Seite, um die Verwendung von DNS und Routen durch das Gerät zu konfigurieren.

DNS-Server (Domain Name System) übersetzen die Namen von Netzwerkgeräten in IP-Adressen (und umgekehrt), d. h., sie ordnen die Namen und Adressen einander zu. Das Gerät sendet in der hier aufgeführten Reihenfolge Anfragen an DNS-Server.

Optionsbeschreibungen

Option	Beschreibung
Serveradresse	Gibt die DNS-Server an. Beim ersten Server in der Liste muss es sich um den schnellsten bzw. zuverlässigsten Server handeln. Falls der erste Server die Anforderung nicht auflösen kann, nimmt das Gerät Kontakt mit dem zweiten Server auf. Falls keiner der Server in der Liste die Anforderung auflösen kann, leitet das Gerät die Anforderung an die DNS-Root-Namenserver im Internet weiter. Wenn DNS-Suchvorgänge (in der Regel auf Port 53) von der Firewall verhindert werden, geben Sie die IP-Adresse eines lokalen Geräts mit Namensauflösungsfunktion an.
Netzwerkadresse	Zeigt die Netzwerkadresse eines Routing-Geräts an.
Maske	Zeigt die Netzwerk-Subnetzmaske an (beispielsweise 255.255.255.0).
Gateway	Gibt die IP-Adressen der anderen Gateways (typischerweise Firewalls oder Router) an, über die das Gerät mit dem Netzwerk kommuniziert. Die Seite **Grundlegende Einstellungen** gibt das Standard-Gateway an.
Messgröße	Zeigt einen Wert an, der von der Routing-Software verwendet wird. Der Standardwert ist 0.0.
Dynamisches Routing aktivieren	Das dynamische Routing erlaubt es Ihren Netzwerkgeräten, einschließlich des Geräts, die Routing-Informationen abzuhören, die Router in Ihrem Netzwerk per Broadcast verbreiten. Die Geräte können anhand dieser Informationen ihre eigenen Routing-Informationen konfigurieren. HINWEIS: Das Gerät unterstützt nur die Routing-Protokolle Routing Information Protocol (RIP) und Open Shortest Path First (OSPF).

Zeiteinstellungen

Auf dieser Seite können Sie die Uhrzeit und das Datum sowie sämtliche Details für die Verwendung von NTP (Network Time Protocol) festlegen. NTP synchronisiert die Uhrzeiten unter den Geräten in einem Netzwerk. Einige Internet-Dienstanbieter bieten einen Uhrzeitdienst an. Weitere Informationen über NTP finden Sie in RFC 1305 unter www.apps.ietf.org/rfc/rfc1305.html, www.ntp.org oder www.ntp.isc.org.

Das Gerät kann seine Uhrzeiteinstellungen mit anderen Geräten synchronisieren, damit seine eigenen Protokolle, Berichte und Zeitpläne stets genau sind. Da NTP-Nachrichten nicht häufig versendet werden, haben sie keinen merklichen Einfluss auf die Leistung des Blade-Servers.

Optionsbeschreibungen

Option	Beschreibung
Zeitzone	Gibt Ihre lokale Zeitzone an. Wenn in Ihrer Region Sommer- und Winterzeit gelten, müssen Sie die Zeitzone zweimal im Jahr ändern.
Systemzeit (lokal)	Gibt das Datum und die lokale Uhrzeit an. Klicken Sie auf das Kalendersymbol, um das Datum festzulegen.
Uhrzeit jetzt einstellen	Wenn Sie darauf klicken, wird die Zeit im Gerät eingestellt. Sie müssen auf diese Schaltfläche klicken, bevor Sie auf **Weiter** klicken. Falls erforderlich, können Sie nach der Installation NTP (Network Time Protocol) konfigurieren.
NTP aktivieren	Wenn ausgewählt, akzeptiert NTP Nachrichten von einem angegebenen Server oder einem Netzwerk-Broadcast.
NTP-Client-Broadcasts aktivieren	Wenn ausgewählt, akzeptiert NTP Nachrichten nur von Netzwerk-Broadcasts. Diese Methode ist hilfreich, wenn das Netzwerk ausgelastet ist, aber anderen Geräten im Netzwerk vertrauen muss. Wenn diese Option nicht ausgewählt ist, akzeptiert NTP Nachrichten nur von Servern, die in der Liste angegeben sind.
NTP-Server	Zeigt die Netzwerkadresse oder einen Domänennamen eines oder mehrerer NTP-Server an, die das Gerät verwendet. Wenn Sie mehrere Server angeben, prüft das Gerät jede NTP-Nachricht, um die richtige Uhrzeit zu bestimmen.

Kennwort

Verwenden Sie diese Seite, um ein Kennwort für das Gerät anzugeben. Ein sicheres Kennwort besteht aus Buchstaben und Ziffern. Sie können bis zu 15 Zeichen eingeben.

Optionsbeschreibungen

Option	Beschreibung
Benutzer-ID	Diese lautet **scmadmin**. Sie können später weitere Benutzer hinzufügen.
Kennwort	Gibt das neue Kennwort an. Ändern Sie das Kennwort baldmöglichst, damit Ihr Gerät geschützt bleibt. Sie müssen das neue Kennwort zweimal eingeben, um es zu bestätigen. Das ursprüngliche Standardkennwort lautet **scmchangeme**. HINWEIS: Sie müssen das Standardkennwort in ein anderes Kennwort ändern, bevor Sie die Konfiguration anwenden können.

▸ Einrichten der Verwaltung durch ePO

Zusammenfassung

Auf dieser Seite können Sie eine Zusammenfassung der Einstellungen anzeigen, die Sie im Setup-Assistenten vorgenommen haben. Wenn Sie einen Wert ändern möchten, klicken Sie auf den entsprechenden blauen Link, um die Seite anzuzeigen, auf der Sie den Wert ursprünglich eingegeben haben.

Nachdem Sie auf **Fertig stellen** geklickt haben, wird der Setup-Assistent abgeschlossen.

Verwenden Sie die auf dieser Seite angezeigte IP-Adresse, um die Benutzeroberfläche aufzurufen. Beispiel: https://192.168.200.10. Beachten Sie, dass die Adresse mit https und nicht mit http beginnt.

Wenn Sie sich zum ersten Mal bei der Benutzeroberfläche anmelden, geben Sie den Benutzernamen **scmadmin** und das Kennwort ein, das Sie in diesem Setup-Assistenten angegeben haben.

Optionsbeschreibungen

Option	Beschreibung
	Der Wert entspricht bewährten Praktiken.
	Der Wert ist wahrscheinlich nicht korrekt. Er ist zwar gültig, entspricht aber nicht bewährten Praktiken. Prüfen Sie den Wert, bevor Sie fortfahren.
	Es wurde kein Wert festgelegt. Der vorgegebene Standardwert wurde nicht geändert. Prüfen Sie den Wert, bevor Sie fortfahren.

▸ Einrichten der Verwaltung durch ePO

Wiederherstellung aus einer Datei

Wenn Sie Ihr Gerät über den Setup-Assistenten innerhalb der Benutzeroberfläche konfigurieren, können Sie mithilfe der Option **Wiederherstellen aus Datei** zuvor gespeicherte Konfigurationsdaten importieren und auf Ihr Gerät übernehmen. Nachdem diese Daten importiert wurden, können Sie Änderungen vornehmen, bevor Sie die Konfiguration anwenden.

Option	Beschreibung
Konfigurationsdatei importieren	Gehen Sie zu einer zuvor gespeicherten Konfigurationsdatei, die Sie auf Ihr Gerät hochladen möchten, und wählen Sie diese aus.
Wiederherzustellende Werte	Standardmäßig wird die gesamte Konfiguration wiederhergestellt. Sie können angeben, dass nur bestimmte Teile Ihrer Konfiguration wiederhergestellt werden sollen, indem Sie die Auswahl der übrigen Daten aufheben. Sie erhalten die Gelegenheit zum Überprüfen dieser Änderungen, bevor sie übernommen werden.
Meldungen beim Importieren der Konfiguration	Beim Importieren der Konfigurationsdatei werden Meldungen angezeigt.

Nach dem Importieren der Konfigurationsdaten wird der benutzerdefinierte Modus des Setup-Assistenten aktiviert. (Siehe Durchführen der benutzerdefinierten Einrichtung.) Alle importierten Optionen werden auf den Assistentenseiten angezeigt, sodass Sie die Möglichkeit zum Vornehmen von Änderungen haben, bevor Sie die Konfiguration übernehmen.

▸ Verwenden der Konfigurationskonsole

Einrichten der Verwaltung durch ePO

Beim Einrichten der Verwaltung durch ePO (nur Email and Web Security Appliances v5.6) enthält der Assistent die folgenden Seiten:

- ePO-Einstellungen
- Grundlegende Einstellungen
- Netzwerkeinstellungen
- Cluster-Verwaltung
- Kennwort
- Zusammenfassung

▸ Verwenden der Konfigurationskonsole
▸ ePO-Einstellungen
▸ Grundlegende Einstellungen
▸ Netzwerkeinstellungen
▸ Cluster-Verwaltung
▸ Kennwort
▸ Zusammenfassung

ePO-Einstellungen

Auf dieser Seite können Sie die ePolicy Orchestrator-Erweiterung und die Hilfe-Erweiterung für Ihre Email and Web Security Appliance herunterladen. Weiterhin können Sie die ePolicy Orchestrator-Verbindungseinstellungen auf Ihre Appliance herunterladen.

Optionsbeschreibungen

Option	Beschreibung
ePO-Erweiterungen	Klicken Sie hier, um die ePolicy Orchestrator-Erweiterungen für Email and Web Security Appliances herunterzuladen. Sie müssen diese Erweiterungen auf Ihrem ePolicy Orchestrator-System installieren.
ePO 4.5-Hilfe	Klicken Sie hier, um die Hilfe-Erweiterung für Email and Web Security Appliances herunterzuladen. Sie müssen diese Erweiterungen auf Ihrem ePolicy Orchestrator-System installieren.
ePO-Verbindungs-einstellungen importieren	Sie müssen diese Verbindungseinstellungen auf Ihren Email and Web Security Appliances importieren, um die Kommunikation zwischen den Appliances und dem ePolicy Orchestrator-Server zu ermöglichen.

▸ Einrichten der Verwaltung durch ePO

Grundlegende Einstellungen

Verwenden Sie diese Seite, um grundlegende Einstellungen für das Gerät anzugeben.

Das Gerät zeigt einige Informationen an, die gelb markiert sind. Um diese Informationen zu ändern, klicken Sie, und geben Sie sie erneut ein.

Optionsbeschreibungen

Option	Beschreibung
Cluster-Modus	• **Aus** – Dies ist eine Standard-Appliance. • **Cluster-Scanner** – Die Appliance empfängt ihre Scan-Arbeit von einer Master-Appliance. • **Cluster-Master** – Die Appliance steuert die Scan-Arbeit verschiedener anderer Appliances. • **Cluster-Failover** – Falls der Master ausfällt, steuert stattdessen diese Appliance die Scan-Arbeit.
Gerätename	Gibt einen Namen an, z. B. Appliance1.
Domänenname	Gibt einen Namen an, z. B. domäne.beispiel.com.
Standard-Gateway (IPv4)	Gibt eine IPv4-Adresse an, z. B. 198.168.10.1. Sie können später testen, ob die Appliance mit diesem Server kommunizieren kann.
Nächster Hop-Router (IPv6)	Gibt eine IPv6-Adresse an, z. B. FD4A:A1B2:C3D4::1.

▸ Einrichten der Verwaltung durch ePO

Netzwerkeinstellungen

Wenn Sie für eine neue Installation zum ersten Mal eine Konfiguration ausführen (oder die Standardeinstellung wiederherstellen), wird die Seite "Netzwerkeinstellungen" angezeigt. Wenn Sie den Cluster-Modus des Geräts ändern, wird diese Seite ebenfalls angezeigt.

Verwenden Sie diese Seite, um die IP-Adresse, die Netzwerkgeschwindigkeiten und den Betriebsmodus für das Gerät zu konfigurieren.

Wenn möglich, füllt das Gerät viele dieser Optionen mithilfe von DHCP aus. Die IP-Adressen müssen eindeutig und für Ihr Netzwerk geeignet sein. Geben Sie nur so viele IP-Adressen wie erforderlich an.

Optionsbeschreibungen

Option	Beschreibung
Netzwerkeinstellungen ändern	Durch Klicken auf diese Option wird ein Assistent mit den folgenden Optionen gestartet.
Betriebsmodus	Bietet eine Auswahl an Modi. Im Modus **Transparenter Router** oder **Transparente Bridge** wissen andere Netzwerkgeräte wie beispielsweise E-Mail-Server nicht, dass der Blade-Server die E-Mail vor dem Weiterleiten abgefangen und gescannt hat. Der Vorgang ist für andere Geräte **transparent**. Im Modus **Expliziter Proxy** senden einige Netzwerkgeräte Datenverkehr an die Appliance. Der Blade-Server fungiert dann als **Proxy** und verarbeitet den Datenverkehr für die Geräte.
LAN-Schnittstellentyp	Gibt den Verbindungstyp an – Kupferleitung oder Glasfaser. Diese Option ist nur für High-Speed-Appliances verfügbar.

Option	Beschreibung
IP-Adresse	Gibt Netzwerkadressen an, die es der Appliance ermöglichen, mit Ihrem Netzwerk zu kommunizieren. Beispiel: 198.168.10.1 oder FD4A:A1B2:C3D4::1. Sie können mehrere IP-Adressen für die Anschlüsse der Appliance angeben. Wenn sich die Appliance im transparenten Modus befindet, werden die IP-Adressen für beide Anschlüsse in einer Liste zusammengefasst. Klicken Sie in den anderen Modi auf "Netzwerk-Schnittstelle 1" bzw. "Netzwerk-Schnittstelle 2", um die jeweilige Liste zu bearbeiten. Konfigurieren Sie die IP-Adresse für die Failover-Appliance. Wenn Sie im Modus "Expliziter Proxy" oder "Transparenter Router" arbeiten, erstellen Sie eine virtuelle IP-Adresse. Die virtuelle IP-Adresse muss für den Master- und den Failover-Management-Blade-Server gleich sein. Bei der ersten IP-Adresse in der Liste handelt es sich um die primäre Adresse. Bei den nachfolgenden IP-Adressen handelt es sich um Aliasadressen.
Netzwerkmaske	Gibt die IPv4-Netzwerkmaske an, z. B. 255.255.255.0, oder gibt die IPv6-Präfixlänge an (1-64 oder 128).

▸ Einrichten der Verwaltung durch ePO

Cluster-Verwaltung

Mithilfe dieser Seite können Sie die Anforderungen an den Lastenausgleich angeben.

- Konfiguration der Cluster-Verwaltung (Standard-Appliance)
- Cluster-Verwaltung (Cluster-Scanner)
- Cluster-Verwaltung (Cluster-Master)
- Cluster-Verwaltung (Cluster-Failover)

Ein *Cluster* ist eine Gruppe von Geräten, die gemeinsame Konfigurationen haben und den Netzwerkverkehr untereinander aufteilen.

Der Cluster kann Folgendes enthalten:

- Einen *Cluster-Master*. Der Master synchronisiert die Konfiguration und verteilt die Last des Netzwerkverkehrs auf die anderen Cluster-Mitglieder.

Weiterhin wird mindestens eines der folgenden Elemente benötigt:

- Ein *Cluster-Failover*. Falls der Cluster-Master ausfällt, übernimmt das Cluster-Failover nahtlos die Arbeit des Cluster-Masters.
- Einen oder mehrere *Cluster-Scanner*. Diese scannen den Datenverkehr gemäß den vom Master synchronisierten Richtlinien.

Beachten Sie, dass der Master und das Failover ebenfalls Datenverkehr scannen können.

Vorzüge

- Eine skalierbare Leistung aufgrund des Lastenausgleichs zwischen mehreren Geräten macht teure Upgrades überflüssig.
- Eine einfachere Verwaltung durch die Synchronisierung von Konfiguration und Aktualisierungen verringert den Verwaltungsaufwand.
- Eine verbesserte Stabilität durch hohe Verfügbarkeit vermindert das Risiko ungeplanter Ausfälle.
- Verbesserte Analyse durch konsolidierte Berichte.

Einrichten des Clusters

Alle Mitglieder des Clusters müssen separat installiert und konfiguriert werden.

Beim Konfigurieren eines Masters oder Failovers muss der Administrator Folgendes tun:

- Für den Proxy-Modus oder den Modus "Transparenter Router" eine virtuelle IP-Adresse festlegen, die für den Master und das Failover gleich ist. Die Cluster-Mitglieder verwenden dann für ein Failover VRRP.
- Für den Modus "Transparente Bridge" den Cluster zur Verwendung von STP im Fall eines Failovers einrichten. Die Bridge-Priorität muss auf dem Master niedriger sein (standardmäßig eingestellt).

Für alle Cluster-Mitglieder muss der Administrator die *Cluster-Kennung* festlegen. Diese eindeutige Kennung stellt sicher, dass die Mitglieder des Clusters korrekt miteinander verbunden werden. Zum Erstellen mehrerer Cluster können Sie für jeden Cluster eine unterschiedliche Kennung verwenden.

Leiten Sie den gesamten zu scannenden Netzwerkverkehr an den Cluster-Master (oder an die virtuelle IP-Adresse, wenn ein Cluster-Failover verwendet wird).

Verwalten des Clusters

Nachdem der Cluster konfiguriert wurde, wird er automatisch mithilfe der Cluster-Kennung verbunden. Das Dashboard des Cluster-Masters zeigt den Geräte- und den Cluster-Typ an.

Der Administrator muss Verwaltungsaufgaben, wie zum Beispiel das Festlegen von Scan-Richtlinien, anschließend nur in der Benutzeroberfläche des Cluster-Masters ausführen. Der Cluster-Master gibt dann diese Konfiguration automatisch an die anderen Cluster-Mitglieder weiter.

Der Cluster-Master fasst Folgendes zusammen:

- Antiviren-Aktualisierungen
- Berichte
- E-Mail in der Warteschlange
- McAfee Quarantine Manager (MQM)

HINWEIS: Software-Patches müssen nacheinander auf jedes einzelne Gerät übernommen werden.

Konfiguration der Cluster-Verwaltung (Standard-Appliance)

Die Cluster-Verwaltung ist deaktiviert.

Cluster-Verwaltung (Cluster-Scanner)

Verwenden Sie diese Seite, um Informationen für eine Scan-Appliance anzugeben.

Option	Beschreibung
Cluster-Kennung	Gibt eine ID an. Der Bereich liegt zwischen 0 und 65535.

Cluster-Verwaltung (Cluster-Master)

Verwenden Sie diese Seite, um Informationen für eine Master-Appliance anzugeben.

Option	Beschreibung
Für Lastenausgleich zu verwendende Adresse	Gibt die Appliance-Adresse an.
Cluster-Kennung	Gibt eine ID an. Der Bereich liegt zwischen 0 und 65535.

Option	Beschreibung
Scannen auf dieser Appliance aktivieren	Wenn diese Option nicht ausgewählt ist, verteilt diese Appliance die gesamte Scan-Arbeitslast auf die Scan-Appliances. HINWEIS: Bei Systemen mit zwei oder drei Appliances ist es sinnvoll, das Scannen auf allen Appliances aktivieren. Bei umfangreicheren Systemen empfiehlt es sich in der Regel, das Scannen nicht auf dem Cluster-Master zu aktivieren.

Cluster-Verwaltung (Cluster-Failover)

Verwenden Sie diese Seite, um Informationen für eine Failover-Appliance anzugeben.

Option	Beschreibung
Für Lastenausgleich zu verwendende Adresse	Gibt die Appliance-Adresse an. Bietet eine Liste aller einer Appliance zugewiesenen Subnetze.
Cluster-Kennung	Gibt eine ID an. Der Bereich liegt zwischen 0 und 65535.
Scannen auf dieser Appliance aktivieren	Wenn diese Option nicht ausgewählt ist, verteilt diese Appliance die gesamte Scan-Arbeitslast auf die Scan-Appliances. HINWEIS: Bei Systemen mit zwei oder drei Appliances ist es sinnvoll, das Scannen auf allen Appliances aktivieren. Bei umfangreicheren Systemen empfiehlt es sich in der Regel, das Scannen nicht auf dem Cluster-Failover zu aktivieren.

▸ Einrichten der Verwaltung durch ePO

Kennwort

Verwenden Sie diese Seite, um ein Kennwort für das Gerät anzugeben. Ein sicheres Kennwort besteht aus Buchstaben und Ziffern. Sie können bis zu 15 Zeichen eingeben.

Optionsbeschreibungen

Option	Beschreibung
Benutzer-ID	Diese lautet **scmadmin**. Sie können später weitere Benutzer hinzufügen.
Kennwort	Gibt das neue Kennwort an. Ändern Sie das Kennwort baldmöglichst, damit Ihr Gerät geschützt bleibt. Sie müssen das neue Kennwort zweimal eingeben, um es zu bestätigen. Das ursprüngliche Standardkennwort lautet **scmchangeme**. HINWEIS: Sie müssen das Standardkennwort in ein anderes Kennwort ändern, bevor Sie die Konfiguration anwenden können.

▸ Einrichten der Verwaltung durch ePO

Zusammenfassung

Auf dieser Seite können Sie eine Zusammenfassung der Einstellungen anzeigen, die Sie im Setup-Assistenten vorgenommen haben. Wenn Sie einen Wert ändern möchten, klicken Sie auf den entsprechenden blauen Link, um die Seite anzuzeigen, auf der Sie den Wert ursprünglich eingegeben haben.

Nachdem Sie auf **Fertig stellen** geklickt haben, wird der Setup-Assistent abgeschlossen.

Verwenden Sie die auf dieser Seite angezeigte IP-Adresse, um die Benutzeroberfläche aufzurufen. Beispiel: https://192.168.200.10. Beachten Sie, dass die Adresse mit https und nicht mit http beginnt.

Wenn Sie sich zum ersten Mal bei der Benutzeroberfläche anmelden, geben Sie den Benutzernamen **scmadmin** und das Kennwort ein, das Sie in diesem Setup-Assistenten angegeben haben.

Optionsbeschreibungen

Option	Beschreibung
	Der Wert entspricht bewährten Praktiken.
	Der Wert ist wahrscheinlich nicht korrekt. Er ist zwar gültig, entspricht aber nicht bewährten Praktiken. Prüfen Sie den Wert, bevor Sie fortfahren.
	Es wurde kein Wert festgelegt. Der vorgegebene Standardwert wurde nicht geändert. Prüfen Sie den Wert, bevor Sie fortfahren.

▸ Einrichten der Verwaltung durch ePO

Testen der Konfiguration

Sie können jetzt die Konfiguration des Geräts testen. In diesem Abschnitt finden Sie Informationen, die Ihnen bei den ersten Schritten helfen:

- Erneutes Starten der Benutzeroberfläche
- Maßnahmen, die das ordnungsgemäße Funktionieren des Geräts sicherstellen

Inhalt

▸ Kennenlernen der Benutzeroberfläche
▸ Testen des Geräts

Kennenlernen der Benutzeroberfläche

Zum Starten der Benutzeroberfläche für das Gerät müssen Sie sich mit dem Benutzernamen und dem Kennwort anmelden. Die Benutzeroberfläche wird auf der Seite **Dashboard** geöffnet.

HINWEIS: Ihre Benutzeroberfläche sieht möglicherweise etwas anders aus als die hier gezeigte Oberfläche, da sie in Abhängigkeit von der Hardware-Plattform, Software-Version und Sprache variieren kann.

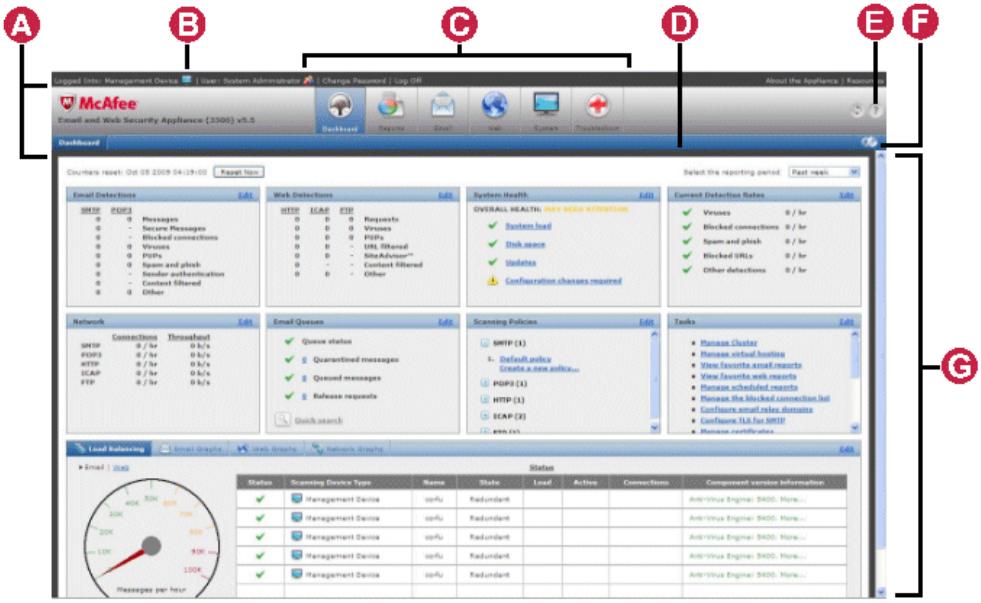


Abbildung 9: Oberflächenkomponenten – Seite "Dashboard"

A	Navigationsleiste	E	Support-Steuerungsschaltflächen
B	Benutzerinformationsleiste	F	Steuerelemente anzeigen
C	Abschnittssymbole	G	Inhaltsbereich
D	Registerkartenleiste		

Navigationsleiste

Die Navigationsleiste umfasst vier Bereiche: Benutzerinformationen, Abschnittssymbole, Registerkartenleiste und Support-Steuerelemente.

Benutzerinformationsleiste

Auf der linken Seite der Benutzerinformationsleiste werden eine Liste der derzeit angemeldeten Benutzer angezeigt (und der Server, bei denen sie angemeldet sind), die Schaltfläche "Kennwort ändern" sowie die Schaltfläche "Abmelden". Auf der rechten Seite der Leiste sehen Sie unter **Info zur Appliance** Informationen zur Appliance- und Paketversion. "Ressourcen" liefert Anweisungen zum Senden einer Virenprobe zur Analyse durch McAfee sowie Links zu weiteren McAfee-Informationsquellen wie dem Serviceportal und der Virus Information Library (Virenbibliothek).

Auf diese Links können Sie über die Benutzerinformationsleiste zugreifen.

Informationen	Produkt- und Lizenzinformationen.

Ressourcen	Kontaktdaten und die folgenden Informationen: **Technischer Support** – Häufig gestellte Fragen auf der McAfee -Website. **Probe übermitteln** – Anweisungen für das Einsenden einer Virenprobe an McAfee. **Vireninformationsbibliothek** – Link zur Vireninformationsbibliothek. Sie enthält detaillierte Informationen zu allen Viren und anderen potenziell unerwünschten Programmen, die von McAfee erkannt und gesäubert werden. **SNMB-Dateien herunterladen** – Herunterladen von Dateien für **SMI**, **MIB** und **HP Openview**.
Schaltfläche "Hilfethemen"	Öffnet die Online-Hilfe.

Abschnittssymbole

Je nach verwendeter Software gibt es fünf oder sechs Abschnittssymbole. Klicken Sie auf ein Symbol, um die Informationen im Inhaltsbereich und in der Registerkartenleiste zu ändern.

Registerkartenleiste

Die Inhalte der Registerkartenleiste werden durch das ausgewählte Abschnittssymbol bestimmt. Die ausgewählte Registerkarte gibt vor, was im Inhaltsbereich angezeigt wird.

Support-Steuerungsschaltflächen

Die Support-Steuerungsschaltflächen sind Aktionen, die für den Inhaltsbereich gelten. Sie heißen (von links nach rechts) "Zurück" und "Hilfe". Es werden zwei weitere Schaltflächen angezeigt, wenn Sie etwas konfigurieren, das es Ihnen erlaubt, Ihre Änderungen zu übernehmen oder zu verwerfen.

Steuerelemente anzeigen

Die Schaltfläche "Steuerelemente anzeigen" aktiviert bzw. deaktiviert ein optionales Statusfenster.

Inhaltsbereich

Der Inhaltsbereich enthält den derzeit aktiven Inhalt. Hier findet die meiste Interaktion statt.

HINWEIS: Die vorgenommenen Änderungen werden wirksam, nachdem Sie auf das grüne Häkchen geklickt haben.

Testen des Geräts

Gehen Sie wie nachfolgend beschrieben vor, um Folgendes zu testen:

- Die Gerätekonfiguration
- E-Mail-Verkehr
- Virenerkennung
- Spam-Erkennung

HINWEIS: Bevor Sie das Gerät verwenden, aktualisieren Sie dessen DAT-Dateien.

Testen der Verbindung

Gehen Sie wie nachfolgend beschrieben vor, um die grundlegende Verbindungsfähigkeit zu bestätigen.

Vorgehensweise

1. Wählen Sie in der Oberfläche **Fehlerbehebung | Tests | Systemtests**.
2. Klicken Sie in der rechten oberen Ecke auf **Start**. Alle Tests sollten erfolgreich sein.

3 Sehen Sie sich den Bereich **Systemtests** an, und prüfen Sie, ob alle Tests erfolgreich waren.

Testen des E-Mail-Verkehrs

Gehen Sie wie nachfolgend beschrieben vor, um sicherzustellen, dass E-Mail-Verkehr durch das Gerät geleitet wird.

Vorgehensweise

1 Senden Sie eine E-Mail von einem externen E-Mail-Konto (wie Hotmail) an einen internen Posteingang, und vergewissern Sie sich, dass die E-Mail angekommen ist.

2 Wählen Sie **Dashboard**.

Im Abschnitt "SMTP-Protokoll" wird angegeben, dass eine Nachricht eingegangen ist.

Testen der Virenerkennung

Gehen Sie wie nachfolgend beschrieben vor, um die Software zu testen, indem Sie die EICAR Standard-Antiviren-Test-Datei ausführen. Diese Datei wurde in Zusammenarbeit mit internationalen Antiviren-Software-Anbietern entwickelt, um einen Standard bereitzustellen, mit dem Kunden die Funktionsfähigkeit ihrer Antiviren-Installationen überprüfen können.

Vorgehensweise

1 Kopieren Sie die folgende Zeile in eine Datei, und achten Sie dabei darauf, dass Sie keine Leerzeichen oder Zeilenumbrüche hinzufügen:
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

2 Speichern Sie die Datei unter dem Namen EICAR.COM.

3 Erstellen Sie von einem externen E-Mail-Konto aus eine Nachricht mit der Datei EICAR.COM als Anhang, und senden Sie die Nachricht an einen internen Posteingang.

4 Kehren Sie zur Seite **Dashboard** zurück.
Im Abschnitt "SMTP-Protokoll" wird angegeben, dass ein Virus erkannt wurde.
Löschen Sie die Nachricht, wenn Sie das Testen Ihrer Installation abgeschlossen haben, damit ahnungslose Benutzer keinen Schreck bekommen.
Diese Datei ist kein Virus. Weitere Informationen zur EICAR-Testdatei finden Sie unter: http://www.eicar.org/.

Testen der Spam-Erkennung

Gehen Sie wie nachfolgend beschrieben vor, um einen *General Test mail for Unsolicited Bulk Email* (Allgemeiner Test auf unerwünschte Bulk-E-Mails, GTUBE) auszuführen, mit dem geprüft wird, ob das Gerät eingehende Spam-Mail erkennt.

Vorgehensweise

1 Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine neue E-Mail.

2 Kopieren Sie den folgenden Text in den Nachrichtenteil der E-Mail:
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-E-Mail*C.34X
Achten Sie darauf, dass der Text keine Zeilenumbrüche enthält.

3 Senden Sie die neue E-Mail an eine interne Posteingangsadresse.

Das Gerät scannt die Nachricht, erkennt sie als Junk-E-Mail und verarbeitet sie entsprechend. Der GTUBE-Test hat Vorrang vor Blacklists und Whitelists.
Nähere Informationen zum GTUBE-Test finden Sie unter http://spamassassin.apache.org/.

Verwenden des Geräts

Lesen Sie diese Informationen, bevor Sie das Gerät verwenden.

Inhalt

- Updates und HotFixes
- Nach der Installation

Updates und HotFixes

Laden Sie vor der Ausbringung des Geräts die neuesten Updates und HotFixes von der Download-Website herunter, und installieren Sie sie:

http://www.mcafee.com/us/downloads/

HINWEIS: Sie benötigen hierfür eine gültige Grant-Nummer.

Nach der Installation

Stellen Sie nach der Installation des Geräts sicher, dass Ihre Konfiguration ordnungsgemäß funktioniert. Siehe Testen des Geräts.

Funktionen der Appliance

In diesem Abschnitt erhalten Sie Informationen zu Vorgehensweisen und Szenarien, die die wesentlichen Vorteile beim Einsatz einer Appliance zum Schutz Ihres Gateways aufzeigen.

Zur Durchführung dieser Vorgehensweisen und Szenarien benötigen Sie einige der Informationen, die Sie in der Konfigurationskonsole und im Setup-Assistenten eingegeben haben.

Vorgehensweise

- Generieren von Berichten

Generieren von Berichten

Das Appliance-Protokoll zeigt Ereignisinformationen für den ausgewählten Berichttyp und den ausgewählten Zeitraum an. Mit den Berichtsfunktionen der Appliance können Sie Berichte erstellen oder Protokolle, Statistiken, Leistungsindikatoren und Diagramme für eine Vielzahl von Daten zu der Appliance und ihren Aktivitäten anzeigen, beispielsweise die Arbeitsspeicher- und Prozessorauslastung.

Nachdem Sie beispielsweise die Schritte unter Testen der Virenerkennung ausgeführt haben, sehen Sie sich den Bereich **Erkennungen** an, wählen Sie **Antiviren-Modul-Erkennungen**, und klicken Sie anschließend auf **Weiter**. Das Protokoll zeigt die EICAR-Testdatei an, die Sie erkannt haben.

Vorgehensweise

Gehen Sie folgendermaßen vor, um die DAT-Dateien der Appliance zu aktualisieren und anschließend den Aktualisierungsbericht zu lesen.

HINWEIS: Die Seite "Systemstatus" wird standardmäßig angezeigt, wenn Sie sich an der Appliance anmelden.

1. Wählen Sie im Navigationsbereich **System | Komponentenverwaltung | Aktualisierungsstatus** aus.
2. Klicken Sie unter **Versionsinformationen und Aktualisierungen** auf **Jetzt aktualisieren** für sämtliche Antiviren- oder Anti-Spam-DAT-Dateiaktualisierungen, die Sie aktualisieren möchten.
3. Kehren Sie zum Navigationsbereich zurück, und wählen Sie **Berichte | Systemberichte** aus.
4. Wählen Sie **Filter**.
5. Wählen Sie als **Ereignistyp** die Option **Aktualisierungen** aus .
6. Klicken Sie auf **Anwenden**. Es werden Informationen zu den Aktualisierungen angezeigt, die auf Ihrer Appliance installiert wurden.

Verwenden von Richtlinien für die Verwaltung von Nachrichten-Scans

Gehen Sie wie nachfolgend beschrieben vor, um die Scan-Funktionen des Blade-Servers in Aktion zu erleben. Sie werden detailliert durch das Erstellen und Testen einiger Beispielrichtlinien geführt und erfahren, wie Sie die relevanten Berichte generieren.

Eine Richtlinie ist eine Zusammenstellung von Einstellungen und Regeln, die dem Blade-Server mitteilt, wie er bestimmte Gefahren für Ihr Netzwerk abwehren soll. Wenn Sie Echtzeitscan-Richtlinien für Ihr Unternehmen erstellen, müssen Sie Ihre Anforderungen in Ruhe analysieren und planen. Sie finden Hinweise für die Richtlinienplanung in der *Online-Hilfe*.

Erstellen einer Antiviren-Scan-Richtlinie

Eine Antiviren-Scan-Richtlinie soll folgende Aktionen umfassen:

- Viren in eingehenden Nachrichten erkennen
- Die Original-E-Mail isolieren
- Den Empfänger benachrichtigen
- Den Absender warnen

Vorgehensweise

Gehen Sie wie nachfolgend beschrieben vor, um zu zeigen, was passiert, wenn eine Mass-Mailer-Virenregel durch die EICAR-Testdatei ausgelöst wird, und welche Aktionen durchgeführt werden können.

1. Stellen Sie auf dem Gerät sicher, dass Sie McAfee Quarantine Manager verwenden (**E-Mail | Quarantänekonfiguration | Quarantäneoptionen**).
2. Wählen Sie auf dem Gerät **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**. Die Standardrichtlinie wird auf **Säubern oder durch Warnung ersetzen** gesetzt, wenn das Säubern fehlschlägt.
3. Klicken Sie auf **Viren: Säubern oder durch Warnung ersetzen**, um die **Standardeinstellungen für Anti-Virus (SMTP)** anzuzeigen.
4. Stellen Sie unter **Aktionen** im Bereich **Wenn ein Virus erkannt wird** sicher, dass **Säuberung versuchen** ausgewählt ist.
5. Wählen Sie im Abschnitt **Und auch** unter der Aktion die Optionen **Benachrichtigungs-E-Mail an Absender zustellen** und **Isolieren der ursprünglichen E-Mail** aus.
6. Wählen Sie unter **Wenn das Säubern fehlschlägt** die Option **Erkanntes Element durch Warnung ersetzen** aus.
7. Wählen Sie im Abschnitt **Und auch** unter **Wenn das Säubern fehlschlägt** die Optionen **Benachrichtigungs-E-Mail an Absender zustellen** und **Isolieren der ursprünglichen E-Mail** als sekundäre Aktionen aus.
8. Klicken Sie auf **OK**.
9. Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien [Scanner-Optionen] – Konfiguration der E-Mail-Adresse**.
10. Weisen Sie unter **Gebouncte E-Mails** die E-Mail-Adresse als Administrator-E-Mail-Adresse zu.

Ohne diese Konfiguration fügt das Gerät keine Absenderadresse zur E-Mail-Benachrichtigung hinzu. Die meisten E-Mail-Server stellen keine E-Mails ohne Absenderadresse zu.

11 Klicken Sie auf **OK** und anschließend auf das grüne Häkchen.

12 Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien [Antivirus] | Benutzerdefinierte Malware-Optionen**.

13 Wählen Sie **Mass-Mailer**, und setzen Sie anschließend **Bei Erkennung** auf **Verbindung verweigern (Blockieren)**.
Der Absender-E-Mail-Server empfängt die Fehlermeldung **Code 550: denied by policy** (Durch Richtlinie verweigert). Das Gerät verwaltet eine Liste der Verbindungen, die unter keinen Umständen E-Mails senden dürfen. Die Liste kann unter **E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails | Listen für Zulassen und Verweigern [+] Zugelassene und blockierte Verbindungen** angezeigt werden. Die Option **Verweigerte Verbindungen** ist in der *Online-Hilfe* beschrieben.

14 So testen Sie die Konfiguration:

- **a** Senden Sie eine E-Mail von <Client-E-Mail-Adresse> an <Server-E-Mail-Adresse>.
- **b** Erstellen Sie eine Textdatei, die folgende Zeichenfolge enthält:
  X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
- **c** Speichern Sie die Datei als eicar.txt.
- **d** Hängen Sie die Datei an die E-Mail an.
  Das Gateway-Sicherheitsgerät ersetzt die Datei durch eine Warnung, und der Absender wird über den Vorgang benachrichtigt.

15 Kehren Sie zu **Benutzerdefinierte Malware-Optionen** zurück, und klicken Sie auf **Spezifischer Erkennungsname:**.

16 Geben Sie EICAR ein.

17 Stellen Sie sicher, dass als primäre Aktion **Daten zurückweisen und Fehlercode zurückgeben (Blockieren)** festgelegt ist, und klicken Sie anschließend auf **OK**.

18 Erstellen Sie von einem externen E-Mail-Konto aus eine Nachricht, und hängen Sie die EICAR-Testdatei an.
Der E-Mail-Client gibt folgende Fehlermeldung zurück: **Code 550: denied by policy** (Durch Richtlinie verweigert).
E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails | Listen für Zulassen und Ablehnen [+] Blockierte Verbindungen ist leer.

19 Ändern Sie unter **Benutzerdefinierte Malware-Optionen** die primäre Aktion in **Verbindung verweigern**, und klicken Sie anschließend auf **OK**.

20 Senden Sie die E-Mail, und überprüfen Sie die verweigerte Verbindung. Sie weist die IP-Adresse Ihres Client-Computers (Beispiel-IP-Adresse) auf.

21 Senden Sie nun eine reguläre E-Mail. Diese wird aufgrund der Liste der verweigerten Verbindungen ebenfalls abgelehnt. Für den Absender-Server scheint es, als ob der Server nicht online wäre.

Das Gerät prüft die Nachricht, wenn diese auf dem E-Mail-Gateway eingeht, und erkennt, dass sie einen Virus enthält. Die Nachricht wird isoliert, und die vorgesehenen Empfänger und der Absender werden darüber benachrichtigt, dass die Nachricht infiziert war.

Erstellen einer Anti-Spam-Scan-Richtlinie

Gehen Sie wie nachfolgend beschrieben vor, um eine Richtlinie zum Schutz Ihres Unternehmens vor dem Empfang unerwünschter Nachrichten einzurichten.

Eine solche Richtlinie schützt Benutzer vor dem Empfang unerwünschter E-Mail-Nachrichten, die ihre Produktivität senken und den Nachrichtenverkehr über Ihre Server erhöhen.

Vorgehensweise

1. Stellen Sie auf dem Gerät sicher, dass Sie McAfee Quarantine Manager verwenden (E-Mail | Quarantänekonfiguration).
2. Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**.
   Sie müssen für die SMTP- und POP3-Protokolle jeweils eine separate Anti-Spam-Richtlinie einrichten.
3. Legen Sie die primäre Aktion auf **Daten akzeptieren und verwerfen** fest.
4. Legen Sie die sekundäre Aktion auf **Original-E-Mail isolieren** fest. Ändern Sie den Spam-Faktor auf 5.
   Wenn Sie die Spam-Erkennung aktivieren, empfiehlt McAfee, auch die Phishing-Erkennung zu aktivieren. Die Scan-Leistung wird durch das gleichzeitige Ausführen von Anti-Spam- und Anti-Phishing-Tests nicht beeinträchtigt.
5. Erstellen Sie von einem externen E-Mail-Konto aus eine Nachricht, und senden Sie sie an einen Posteingang, der durch das Gerät geschützt wird.
6. Geben Sie folgenden Nachrichtentext ein:
   XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-E-Mail*C.34X
7. Senden Sie die Nachricht.
8. Öffnen Sie McAfee Quarantine Manager, und sehen Sie sich die Spam-Warteschlange an.
9. Geben Sie die Spam-Nachricht aus der Quarantäne frei.
10. Überprüfen Sie, ob die Nachricht im E-Mail-Konto des Empfängers eingegangen ist.

Erkannte Nachrichten werden an McAfee Quarantine Manager gesendet und können von einem Administrator verwaltet werden.

Erstellen einer E-Mail-Compliance-Richtlinie

Gehen Sie wie nachfolgend beschrieben vor, um eine Richtlinie zu erstellen, die sicherstellt, dass die von Ihren Benutzern an externe E-Mail-Konten gesendeten Nachrichten den offiziellen Inhaltsbibliotheken entsprechen.

Diese Richtlinie gewährleistet die Einhaltung gesetzlicher Standards, wie dem HIPAA-Standard für den Schutz persönlicher medizinischer Informationen und Datenschutzstandards zu Nachrichten mit vertraulichen Informationen. Sie benachrichtigt Absender darüber, falls ihre Nachrichten die Compliance-Anforderungen nicht erfüllen.

Vorgehensweise

1. Wählen Sie auf dem Gerät **E-Mail | E-Mail-Richtlinien | Wörterbücher**.
2. Wählen Sie **Datenschutzregeln**.
3. Zeigen Sie die **Liste der Begriffe für das ausgewählte Wörterbuch** an.
4. Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**.
5. Wählen Sie unter **Inhalt** die Option **Inhalts-Scans**.
6. Wählen Sie **Inhalts-Scans aktivieren | Ja**.
7. Klicken Sie auf **OK**.

8 Klicken Sie unter **Regeln für Inhalts-Scans** auf **Erstellen einer neuen Regel für Inhalts-Scans**.

9 Wählen Sie **Datenschutzregeln** unter **Typ: Compliance**.

10 Klicken Sie auf **OK**.

11 Wählen Sie unter **Falls ausgelöst** die Option **Daten akzeptieren und verwerfen (Blockieren)** aus.

12 Klicken Sie auf **OK**.

13 Klicken Sie auf **OK**.

14 Erstellen Sie eine E-Mail auf dem Server von <Beispiel-Server-E-Mail-Adresse> an <Beispiel-Client-E-Mail-Adresse>. Geben Sie folgenden Text ein: Hallo: Wir müssen den bestätigten Wert Ihrer Rente berechnen. Falls sich herausstellt, dass Ihre Anlagen über weniger Kapital verfügen als erwartet, sollten Sie eine Schlichtungsstelle anrufen.

15 Senden Sie die Nachricht.

16 Unter **E-Mail | E-Mail-Übersicht | ZUSAMMENFASSUNG FÜR EINGEHENDE E-MAILS** können Sie die Ergebnisse ansehen.

Der Client-E-Mail-Agent erhält die E-Mail nicht. Das Server-E-Mail-Konto sollte zwei E-Mail-Nachrichten erhalten: eine E-Mail-Benachrichtigung, dass die Nachricht den Compliance-Test nicht bestanden hat, und eine Kopie der ursprünglichen E-Mail.

Erstellen einer Richtlinie für die Inhaltsfilterung

Gehen Sie wie nachfolgend beschrieben vor, um eine Richtlinie für die Isolierung eingehender Nachrichten zu erstellen, die unerwünschten Inhalt enthalten. Dies erfolgt nun mithilfe eines Assistenten, der Sie durch den Vorgang führt.

Gehen Sie wie folgt vor, um ein Beispiel für die Inhaltsfilterung einzurichten:

Vorgehensweise

1 Wählen Sie auf dem Gerät **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**.
Wenn Inhalts-Scans deaktiviert sind, wählen Sie **Ja** unter **Inhalts-Scans aktivieren**.

2 Klicken Sie im Abschnitt **Inhalt** auf **Inhalts-Scans**.
Wenn Inhalts-Scans derzeit deaktiviert sind, klicken Sie auf **Ja**.

3 Geben Sie unter **Regelname:** einen Regelnamen ein.

4 Klicken Sie auf **Weiter >**.

5 Wählen Sie unter **Die Regel wird ausgelöst, wenn eines der ausgewählten Wörterbücher zutrifft** eines oder mehrere Wörterbücher aus, zum Beispiel **Glücksspiel (Englisch)**.

6 Klicken Sie auf **Weiter >**.

7 Wählen Sie unter **Die Regel wird ignoriert, wenn eines der ausgewählten Wörterbücher zutrifft** alle Wörterbücher aus, die ignoriert werden sollen. Wählen Sie für dieses Beispiel keines der Wörterbücher aus.

8 Klicken Sie auf **Weiter >**.

9 Wählen Sie unter **Wenn die Regel für Inhalts-Scans ausgelöst wird** die für Ihre Zwecke erforderliche Aktion aus, zum Beispiel **Inhalt durch Warnung ersetzen (Bearbeiten)**.

10 Wählen Sie im Bereich **Ursprüngliche E-Mail** die Option **Isolieren** aus.

11 Klicken Sie auf **Fertig stellen**.

12 Klicken Sie auf **OK**, um den Assistenten abzuschließen.

13 Wenden Sie Ihre Konfigurationsänderungen an.

14 Erstellen Sie von einem externen E-Mail-Konto aus eine Nachricht, und senden Sie sie an einen Test-Posteingang, der durch das Gerät geschützt wird. Geben Sie folgenden Nachrichtentext ein: Wir sehen uns heute Abend beim Blackjack!

15 Senden Sie die Nachricht.

16 Öffnen Sie den Posteingang, an den Sie die Nachricht adressiert haben, und zeigen Sie die Warnung an.

17 Unter **E-Mail | E-Mail-Übersicht | ZUSAMMENFASSUNG FÜR EINGEHENDE E-MAILS** können Sie das Ereignis ansehen.

18 Rufen Sie das **Dashboard** auf, um Informationen zu Elementen einzusehen, die aufgrund ihres Inhalts isoliert wurden.

19 Öffnen Sie unter Verwendung des E-Mail-Kontos des Empfängers die Benutzeroberfläche von McAfee Quarantine Manager, und wählen Sie **Unerwünschter Inhalt**.

20 Wählen Sie die Nachricht aus, und klicken Sie auf **Übermitteln für Freigabe**.

21 Öffnen Sie die Administratoroberfläche von McAfee Quarantine Manager, und wählen Sie **Übermittlungen durch Benutzer**.

22 Wählen Sie **Für Freigabe übermittelt**.

23 Wählen Sie die Nachricht aus, und klicken Sie auf **Freigeben**.

24 Öffnen Sie den Posteingang, an den Sie die Nachricht adressiert haben, und zeigen Sie die erhaltene Nachricht an.

Das Gerät prüft die Nachricht, wenn diese auf dem E-Mail-Gateway eingeht, und erkennt, dass sie einen Virus enthält. Das Gerät isoliert die Nachricht und benachrichtigt den vorgesehenen Empfänger und den Absender darüber, dass die Nachricht infiziert war.

Informationen zum Verwalten virtueller Hosts

Bei der Verwendung von virtuellen Hosts kann sich ein einzelnes Gerät wie mehrere Geräte verhalten. Jedes *virtuelle* Gerät kann den Datenverkehr innerhalb von angegebenen IP-Adressbereichen verwalten, indem es dem Gerät ermöglicht, Scan-Dienste für den Datenverkehr von vielen Quellen oder Kunden anzubieten.

Vorzüge

- Trennt den Datenverkehr der einzelnen Kunden voneinander.
- Für jeden Kunden oder Host können Richtlinien erstellt werden, was die Konfiguration vereinfacht und Konflikte verhindert, die bei komplexen Richtlinien auftreten können.
- Berichte sind für jeden Kunden oder Host einzeln verfügbar, wodurch die Notwendigkeit einer komplexen Filterung entfällt.
- Falls das Gerät verhaltensbedingt auf eine Reputation-Blacklist gesetzt wird, betrifft dies nur einen virtuellen Host und nicht das gesamte Gerät.

Einrichten der virtuellen Hosts

Die Funktion steht nur für SMTP-Scans zur Verfügung. Informationen zur Angabe des Pools der IP-Adressen für den eingehenden Datenverkehr und des optionalen Pools der Adressen für den ausgehenden Datenverkehr finden Sie auf der Seite **System | Virtuelles Hosting | Virtuelle Netzwerke**.

Verwalten der virtuellen Hosts

Funktion	Verhalten
E-Mail-Richtlinie	Jeder virtuelle Host besitzt eine eigene Registerkarte, auf der Sie die Scan-Richtlinien für den Host erstellen können.
E-Mail-Konfiguration	Jeder virtuelle Host besitzt eine eigene Registerkarte, auf der Sie spezielle MTA-Funktionen für den jeweiligen Host konfigurieren können.
E-Mail in der Warteschlange	Sie können alle in der Warteschlange befindlichen E-Mails oder nur die in der Warteschlange befindlichen E-Mails für die einzelnen Hosts anzeigen.
Isolierte E-Mails	Sie können alle isolierten E-Mails oder nur die isolierten E-Mails für die einzelnen Hosts anzeigen.
Berichterstellung	Sie können alle Berichte oder nur die Berichte für die einzelnen Hosts anzeigen.

Verhalten zwischen dem Gerät und MTAs

Wenn das Gerät E-Mails empfängt, die an den IP-Adressbereich des virtuellen Hosts gesendet wurden, führt der virtuelle Host Folgendes aus:

- Er reagiert mit einem eigenen SMTP-Willkommensbanner auf die SMTP-Konversation.
- Er fügt optional seine eigenen Adressinformationen zum Header "Received" hinzu.
- Er scannt die E-Mails gemäß seiner eigenen Richtlinie.

Wenn das Gerät E-Mails zustellt, geschieht Folgendes:

- Die IP-Adresse wird einem Adresspool für ausgehenden Datenverkehr entnommen, oder es wird eine physische IP-Adresse verwendet, wenn kein entsprechender Adresspool angegeben wurde.
- Der empfangende Mailübertragungsagent (MTA) sieht die IP-Adresse des virtuellen Hosts.
- Wenn ein Adresspool vorhanden ist, wird die IP-Adresse nach dem Round-Robin-Verfahren ausgewählt.
- Die EHLO-Antwort wird an den virtuellen Host ausgegeben.

Fehlerbehebung

In diesem Abschnitt sind Lösungen zu Problemen enthalten, die beim Installieren und Ausführen der Appliance auftreten können, sowie Antworten zu häufig gestellten Fragen (FAQs).

- Allgemeine Probleme
- Häufig gestellte Fragen
- Weitere Hilfe – Die Link-Leiste

Allgemeine Probleme

In diesem Abschnitt werden einige allgemeine Probleme erläutert.

Die Appliance wird nicht mit Strom versorgt

Stellen Sie sicher, dass das Gerät über die richtigen Kabel ordnungsgemäß an eine funktionierende Steckdose angeschlossen ist. Falls die Netzsteckdose mit einem Schalter ausgestattet ist, muss sie eingeschaltet sein.

Falls die Appliance immer noch nicht mit Strom versorgt wird, überprüfen Sie die Steckdose, indem Sie ein anderes Gerät anschließen. Funktioniert die Steckdose, liegt das Problem bei der Appliance oder dem Netzkabel zur Appliance. Wenden Sie sich an den Händler.

Die Appliance empfängt keinen Datenverkehr aus dem Netzwerk

Überprüfen Sie Folgendes:

- Die Appliance ist eingeschaltet und die Software wird ausgeführt.

  Wenn die LED des Netzschalters orange leuchtet, ist die Appliance angeschlossen, aber nicht eingeschaltet. Bei eingeschalteter Appliance leuchtet die LED des Netzschalters grün.

- Die Netzwerkkabel sind unbeschädigt und ordnungsgemäß an die Anschlüsse der Appliance und die vorhandenen Netzwerkkomponenten angeschlossen. Falls Sie nicht die im Lieferumfang der Appliance enthaltenen Kabel verwendet haben, stellen Sie sicher, dass Ihre Kabel der richtigen Spezifikation entsprechen.
- Ihre Netzwerkgeräte sind an die korrekten LAN-Anschlüsse der Appliance angeschlossen.
- Die Geschwindigkeiten der Netzwerkkarte und die Einstellungen für Voll- oder Halb-Duplex auf beiden Seiten der Verbindungen sind kompatibel, und die Einstellungen wurden korrekt automatisch ausgehandelt.
- Die LAN-LEDs leuchten.

Falls die Appliance immer noch keinen Netzwerkverkehr empfängt, überprüfen Sie die Netzwerkkabel und die Netzwerkanschlüsse an Ihren Netzwerkgeräten. Funktionieren Kabel

und Anschlüsse ordnungsgemäß, liegt das Problem bei der Appliance. Wenden Sie sich an den Händler.

Häufig gestellte Fragen

In diesem Abschnitt werden einige der Probleme erläutert, die beim Integrieren Ihrer Appliance in das bereits vorhandene Netzwerk auftreten können.

Probleme mit der Benutzeroberfläche

Dieser Abschnitt beinhaltet Lösungen zu Problemen, die beim Konfigurieren der Appliance über die Benutzeroberfläche auftreten können.

Warum gelange ich mit der Browser-Schaltfläche "Zurück" wieder zum Anmeldefenster?

Dies ist ein bekanntes Problem, das bei Verwendung der Webbrowser-Version der Appliance-Software auftritt. Verwenden Sie stattdessen die Appliance-Anwendung.

Ich kann nicht auf das Anmeldefenster zugreifen.

Überprüfen Sie Folgendes:

- Die Appliance ist eingeschaltet, und die Software wird ausgeführt. Das wird durch die leuchtende LED des Netzschalters und die nicht leuchtenden LEDs der Festplattenlaufwerke angezeigt.
- Sie haben im Adressfeld Ihres Webbrowsers **https** (und nicht **http**) verwendet. Stellen Sie sicher, dass Ihr Browser SSL-Verschlüsselung (SSL – Secure Sockets Layer) unterstützt und diese aktiviert ist.
- Auf dem Computer, mit dem Sie die Appliance verwalten, ist die Appliance nicht als dessen Proxy konfiguriert. Falls Sie zwischen dem Verwaltungscomputer und der Appliance einen Proxy haben, muss die Appliance als Übergabe-Host des Proxys konfiguriert werden.
- Falls Sie über den LAN1-Anschluss eine Remote-Verbindung zur Appliance über das Netzwerk haben, überprüfen Sie Folgendes:
  - Der verwendete Computer hat eine funktionstüchtige Verbindung zu Ihrem Netzwerk und kann dasselbe Subnetz erreichen, mit dem auch die Appliance verbunden ist.
  - Sie haben im URL-Feld des Webbrowsers die neue IP-Adresse verwendet, die Sie für den LAN1-Anschluss konfiguriert haben. Verwenden Sie die Standard-IP-Adresse 10.1.1.108, sofern Sie sie nicht deaktiviert oder gelöscht haben (https://10.1.1.108).

    Die IP-Adresse der Appliance muss für das Subnetz geeignet sein, mit dem die Appliance verbunden ist. Ist sie nicht geeignet, versuchen Sie es mit der Standard-IP-Adresse. Führt dies ebenfalls nicht zum Erfolg, versuchen Sie es über eine direkte Verwaltungsverbindung.

    HINWEIS: Über den LAN2-Anschluss erhalten Sie nur eine direkte Verwaltungsverbindung, wenn Sie die Appliance im Modus "Expliziter Proxy" verwenden und den LAN2-Anschluss nicht deaktiviert haben.

  - Die Appliance hat eine funktionierende Verbindung zu Ihrem vorhandenen Netzwerk, die durch die blinkende NIC-1-LED für Netzwerkaktivität in der Benutzeroberfläche angezeigt wird.

Blinken die LEDs nicht, stellen Sie sicher, dass das verwendete Kabel unbeschädigt und ordnungsgemäß an den LAN1-Anschluss der Appliance sowie an Ihre vorhandenen Netzwerkgeräte angeschlossen ist. Falls Sie nicht das mit der Appliance gelieferte blaue Kabel verwendet haben, stellen Sie sicher, dass das Kabel ein durchgängiges (ungekreuztes) UTP-Netzwerkkabel ist.

- Wenn die Appliance im Modus "Expliziter Proxy" arbeitet und Sie eine direkte lokale Verwaltungsverbindung über den LAN2-Anschluss haben, überprüfen Sie Folgendes:
  - Der LAN2-Anschluss ist nicht deaktiviert. Stellen Sie eine Remote-Verbindung her, um dies zu überprüfen.
  - Sie haben in das URL-Feld Ihres Webbrowsers die neue IP-Adresse eingegeben, die Sie für den LAN2-Anschluss konfiguriert haben (die Standardadresse lautet 10.1.2.108).
  - Die Appliance hat eine funktionierende Verbindung zu Ihrem Computer, die durch die blinkende NIC-2-LED für Netzwerkaktivität im Bedienfeld angezeigt wird.

    Blinkt die LED nicht, stellen Sie sicher, dass das verwendete Kabel unbeschädigt und ordnungsgemäß an den LAN2-Anschluss der Appliance sowie an den Netzwerkanschluss Ihres Computers angeschlossen ist. Falls Sie nicht das mit der Appliance gelieferte orangefarbene Kabel verwendet haben, stellen Sie sicher, dass das Kabel ein gekreuztes UTP-Netzwerkkabel ist.

Mein Kennwort ist ungültig.

Wenn Sie kürzlich die Software der Appliance wiederhergestellt haben, ohne die vorherigen Einstellungen beibehalten zu haben, wird das Verwaltungskennwort auf das Standardkennwort **scmchangeme** zurückgesetzt.

Ich habe mein Kennwort vergessen.

Verwenden Sie die Wiederherstellungs-CD der Appliance, um das Kennwort der Appliance auf die Standardkennwörter scmchangeme usnd dlpchangeme zurückzusetzen.

Ein Teil der Benutzeroberfläche wird nicht korrekt angezeigt.

Die Benutzeroberfläche der Appliance ist für Internet Explorer 6.0 oder höher (unter Windows) sowie für Mozilla Firefox 2.0 (unter Linux) vorgesehen. Überprüfen Sie in den beigefügten Versionshinweisen, ob es bei der Verwendung einiger Webbrowser auf bestimmten Betriebssystemen Probleme gibt.

Client(-Software) kann nicht über die Appliance kommunizieren.

Überprüfen Sie Folgendes:

- Die korrekten Protokolle für die Appliance sind aktiviert (standardmäßig sind alle Protokolle aktiviert).
- Die Clients und andere Geräte sind so konfiguriert, dass sie den Datenverkehr an die Appliance und von der Appliance leiten.
- Es bestehen keine Netzwerkprobleme, und Ihr Gerät ist ordnungsgemäß angeschlossen.

Webbrowsing funktioniert nicht, oder URL-Blockierung wird nicht durchgesetzt.

Die Appliance muss Zugriff auf einen DNS-Server haben, um Webbrowsing-Anfragen (über HTTP) überprüfen zu können und zu ermitteln, welche URLs blockiert werden sollen, falls das Blockieren von URLs konfiguriert ist.

E-Mail-Probleme

In diesem Abschnitt werden E-Mail-Probleme erläutert.

Anti-Relay funktioniert nicht.

So aktivieren Sie die Anti-Relay-Funktion:

1. Klicken Sie im Navigationsbereich auf **Konfigurieren | SMTP**.
2. Wählen Sie **Protokolleinstellungen | Anti-Relay-Einstellungen** aus.
3. Geben Sie unter **Lokale Domänen** mindestens eine lokale Domäne an. Andernfalls ist die Appliance vor Weiterleitungen und Missbrauch durch Spammer von außerhalb Ihres Netzwerks ungeschützt.

Warum kann ich nicht nur den Namen des Absenders angeben, für den ich das Relay blockieren möchte?

Sie müssen sich das Anti-Relay als eine Blockierung zwischen zwei Systemen vorstellen, Anti-Spam hingegen als eine absenderbasierte Blockierung.

Das Anti-Relay wird mithilfe der Domänen und Netzwerke konfiguriert, für die die Appliance E-Mails überträgt. Die Anti-Spam-Konfiguration blockiert eine Nachricht jedoch basierend auf deren Absender.

Die Directory Harvest-Prävention funktioniert nicht.

Damit die Directory Harvest-Prävention (DHA) ordnungsgemäß funktioniert, muss der E-Mail-Server während der SMTP-Kommunikation eine Überprüfung auf gültige Empfänger durchführen und anschließend einen Non-Delivery-Report senden.

Einige E-Mail-Server senden keine Fehler vom Typ "Unbekannter Benutzer" als Teil der SMTP-Konfiguration. Dazu gehören u. a. die folgenden Server:

- Microsoft Exchange 2000 und 2003 (wenn die Standardkonfiguration verwendet wird)
- Qmail
- Lotus Domino

Schlagen Sie in der Benutzerdokumentation des E-Mail-Servers nach, ob der E-Mail-Server so konfiguriert werden kann, dass er den Bericht "550 Recipient address rejected: User unknown" (Empfängeradresse nicht akzeptiert: Unbekannter Benutzer) als Teil der SMTP-Kommunikation sendet, wenn eine Nachricht an einen unbekannten Benutzer gefunden wird.

Mit der LDAP-Integration kann dieses Problem umgangen werden. Weitere Informationen finden Sie im Produkthandbuch zu Ihrer Version der McAfee Email and Web Security Appliance.

Zustellung

In diesem Abschnitt werden Probleme bei der Zustellung beschrieben.

Warum werden die Nachrichten nicht gesendet, wenn ich im Ordner "Zurückgestellte E-Mail" die Option "Alle erneut senden" auswähle?

Wählen Sie nach der Auswahl von **Alle erneut senden** die Option **Aktualisieren**, um anzuzeigen, wie weit die Appliance in der Bearbeitung der Nachrichtenliste fortgeschritten ist.

Die Appliance verarbeitet die Nachrichten, bis alle gesendet wurden. Falls danach noch immer ein durch das Netzwerk oder eine Fehlkonfiguration der Appliance verursachtes

Übertragungsproblem besteht, wird die Nachricht in den Ordner "Zurückgestellte E-Mail" zurückgeleitet.

Die Appliance versucht jeweils alle 30 Minuten, sämtliche zurückgestellten Nachrichten zu senden.

Welche Einstellungen kann ich überprüfen, wenn Probleme bei der E-Mail-Zustellung auftreten?

Wenn die E-Mail über DNS zugestellt werden soll, muss in der Benutzeroberfläche die Option **DNS** ausgewählt sein.

Falls Ihr interner Mail-Server keine eingehenden E-Mails empfängt, überprüfen Sie, ob dieser Mail-Server so konfiguriert ist, dass er E-Mails von der Appliance akzeptiert.

Geben Sie in der Liste der lokalen Domänen für die E-Mail-Zustellung keine allgemeine Regel mit Platzhaltern an. Aktivieren Sie stattdessen das Fallback-Relay, und legen Sie sie dort fest.

E-Mail-Anhänge

In diesem Abschnitt werden Probleme mit E-Mail-Anhängen erläutert.

Die Appliance blockiert alle E-Mails, wenn ich die Anzahl der Anhänge verringere, ab der blockiert werden soll.

Diese Einstellung soll E-Mail-Nachrichten mit einer großen Zahl von Anhängen blockieren, die zu viel Bandbreite belegen.

Einige E-Mail-Clients (z. B. Outlook Express) speichern zusätzliche Informationen in zusätzlichen Anhängen und betten sogar den Hauptnachrichtentext in einen Anhang ein.

Wenn diese Zahl zu niedrig gewählt ist, werden u. U. sogar reguläre E-Mail-Nachrichten abgelehnt.

EICAR (der Testvirus) oder Inhalt, der blockiert werden muss, gelangt immer noch durch.

Stellen Sie sicher, dass sich die Appliance wirklich im Mail-Pfad befindet. Untersuchen Sie die Header einer E-Mail-Nachricht (wählen Sie in Outlook **Ansicht | Optionen | Internetkopfzeilen**).

Wenn sich die Appliance im Mail-Pfad befindet, wird eine Kopfzeile der Form **Received: from Absender by Servername via ws_smtp** angezeigt, wobei **Absender** und **Servername** durch den Namen des tatsächlichen Absenders und den Namen der Appliance ersetzt werden.

Wenn die Appliance einen Virus erkennt, erhalte ich eine Benachrichtigung über eine Inhaltsverletzung.

Dieses Problem kann durch einen Konflikt zwischen der Warnhinweisseite der HTML-Vorlage und einer Inhalts-Scan-Regel verursacht werden.

Es kann dann auftreten, wenn Sie beispielsweise den Inhalt nach dem Wort **Virus** filtern, gleichzeitig aber die HTML-Vorlage für die Virenerkennung so eingerichtet haben, dass sie eine Warnmeldung über einen erkannten Virus ausgibt. Eine eingehende Nachricht mit einem Virus bewirkt dann, dass die Nachricht durch die Meldung **Ein Virus wurde erkannt** ersetzt wird. Die Ersatzmeldung läuft daraufhin durch den Inhaltsfilter, der durch das Wort **Virus** ausgelöst wird, und die Meldung wird dann durch eine Inhaltsverletzung anstelle einer Virenbenachrichtigung ersetzt.

Warum kommen E-Mails von einigen Absendern an, während andere blockiert werden?

Überprüfen Sie die Konfiguration der internen und externen Netzwerke. Achten Sie darauf, dass die Liste der externen Netzwerke als letzten Eintrag ein Sternchen (*) enthält. Vergewissern Sie sich zudem, dass die Liste der internen Netzwerke kein Sternchen aufweist.

POP3

In diesem Abschnitt werden POP3-Probleme erläutert.

Ich habe eine dedizierte POP3-Verbindung eingerichtet, und POP3 funktioniert nicht mehr.

Der allgemeine und der dedizierte Server dürfen nicht denselben Port verwenden. Die Standard-Port-Nummer für POP3 lautet 110. Der dedizierte Server setzt den allgemeinen Server außer Kraft.

Wenn ich E-Mails mit Outlook Express über POP3 abrufe, erhalte ich manchmal eine Zeitüberschreitungsmeldung mit den Optionen "Abbrechen" oder "Warten".

Die Appliance muss die gesamte E-Mail-Nachricht herunterladen und scannen, bevor sie sie an Outlook Express weiterleiten kann. Bei einer großen Nachricht oder einem langsamen E-Mail-Server kann dies einige Zeit in Anspruch nehmen. Klicken Sie auf **Warten**, um Outlook Express zum Warten zu zwingen, bis die Appliance die Nachricht verarbeitet hat.

Ich erhalte gelegentlich POP3-Mail-Nachrichten doppelt.

Einige E-Mail-Clients gehen nicht korrekt mit Zeitüberschreitungen um. Wenn die Appliance eine sehr große Nachricht herunterlädt und scannt, kann beim Client während des Wartens auf eine Antwort eine Zeitüberschreitung eintreten.

Sie werden dann in einem Popup-Fenster aufgefordert, zu warten oder das Herunterladen abzubrechen. Wenn Sie **Abbrechen** wählen und einen zweiten Download starten, kann sich die Nachricht zwei Mal in Ihrem Posteingang befinden.

Physische Konfiguration

In diesem Abschnitt werden Probleme mit der physischen Konfiguration erläutert.

Ich habe die Appliance mit dem Netzwerk verbunden, kann jedoch mit meinem Browser keine Verbindung zu ihr herstellen.

Vergewissern Sie sich im Modus "Expliziter Proxy", dass Sie den LAN1-Adapter an Ihr Netzwerk angeschlossen haben. LAN2 dient nur zur Verwaltung und muss direkt an einen Laptop oder Computer angeschlossen werden.

In meinem Netzwerk sind zwei Appliances vorhanden, ich kann mich aber nur an einer anmelden.

Wenn Sie eine Appliance installiert oder kürzlich die Option "Konfiguration wiederherstellen" verwendet haben, ist es möglich, dass zwei oder mehr Appliances in Ihrem Netzwerk über die dieselbe Standard-IP-Adresse verfügen.

Um sicherzustellen, dass alle Appliances über eindeutige IP-Adressen verfügen, können Sie Folgendes verwenden:

- Den Setup-Assistenten
- Die Netzwerkeinstellungen
- Die Konfigurationskonsole

Systemkonfiguration

In diesem Abschnitt werden Probleme mit der Systemkonfiguration erläutert.

Ich habe unterschiedliche Regeln für eingehenden und ausgehenden Datenverkehr erstellt. Wenn ich E-Mails empfange oder auf externen Websites surfe, wird die Regel für ausgehenden und nicht die für eingehenden Datenverkehr ausgelöst.

Vergewissern Sie sich, dass die IP-Adresse der Firewall in der Liste der externen Netzwerke aufgeführt ist. Verbindungen von außen erscheinen der Appliance dann so, als kämen sie von der Firewall.

Systemverwaltung

In diesem Abschnitt werden Probleme mit der Systemverwaltung erläutert.

Die Appliance nimmt die HotFix-Datei nicht an.

Dekomprimieren Sie die HotFix-Datei nicht, bevor Sie sie auf die Appliance hochladen. Die Appliance akzeptiert die Originaldatei so, wie Sie sie empfangen haben – nämlich mit der Erweiterung TGZ.

Wie kann ich die Größe der Protokolldateien der Appliance steuern?

Die Appliance speichert ihre Protokolldateien in einem textähnlichen Format (XML) auf einer Partition (/log) ihrer internen Festplatte. Standardmäßig werden die Protokolle nach einigen Tage geleert. Die Appliance gibt eine Warnung aus, wenn ihre Bereiche beinahe gefüllt sind, in der Regel bei 75 % und bei 90 %.

- Die prozentuale Belegung der Protokollpartition erfahren Sie im Navigationsbereich über **Überwachen | Status**. Klicken Sie auf **Einstellungen**, um die Anzeigefarben anzupassen.
- Zum Leeren des Protokolls wählen Sie **Konfigurieren | Protokollierung, Warnungen und SNMP**, und wählen Sie dann im Navigationsbereich unter **Kanaleinstellungen** die Registerkarte **XML**.
- Zur Einstellung der Warnstufen wählen Sie im Navigationsbereich **Überwachen | Ressourcen** und dann **Datenträgerauslastung**.

Automatische Aktualisierung der Antiviren-Software

In diesem Abschnitt werden Probleme bei den automatischen Aktualisierungen der Antiviren-Software erläutert.

Wenn ich eine sofortige Aktualisierung anfordere, geschieht nichts. Wie kann ich erkennen, ob die DAT-Datei aktualisiert wurde?

So zeigen Sie die Versionsnummer der installierten DAT-Datei an:

- Klicken Sie im Navigationsbereich auf **Überwachen | Systemstatus** und dann auf **Allgemeiner Status**.

- Sie können auch **Überwachen | Updates** auswählen.

Die DAT-Dateien werden heruntergeladen, geprüft und angewendet.

Die Appliance wartet nicht, bis die Aktualisierung vollständig durchgeführt worden ist (dies kann auch bei einer schnellen Internetverbindung einige Minuten dauern), sondern startet sie im Hintergrund.

Wählen Sie **Überwachen | Systemstatus**, um nach der Installation der neuen DAT-Dateien auf der nächsten Seite die neue DAT-Versionsnummer anzuzeigen.

Anti-Spam

In diesem Abschnitt werden Probleme mit dem Spam-Schutz erläutert.

Ich kann die in diesem Handbuch beschriebenen Anti-Spam-Funktionen nicht finden.

Für einige Anti-Spam-Funktionen muss das Anti-Spam-Modul aktiviert werden.

Ich habe die Appliance so konfiguriert, dass Spam-Mail durch eine RBL-Server-Überprüfung abgelehnt wird, aber einige Spam-Mails kommen dennoch an.

Es gibt keine Anti-Spam-Software, die sämtliche Spam-E-Mails erkennen und blockieren kann. Die Appliance verwendet eine Liste der Namen von bekannten Personen, die E-Mail-Missbrauch betreiben, sowie der von ihnen benutzten Netzwerke.

Diese Listen verringern die Anzahl unerwünschter E-Mails zwar wirksam, sind aber nicht vollständig.

So blockieren Sie einen bestimmten Spam-Absender:

1. Klicken Sie im Navigationsbereich auf **Konfigurieren | SMTP**.
2. Wählen Sie **Protokolleinstellungen | Einstellungen für Zulassen und Verweigern**.
3. Geben Sie unter **Absender verweigern** die E-Mail-Adresse des Absenders ein.

Benutzer erhalten keine regulären E-Mail-Nachrichten.

Benutzer empfangen möglicherweise aus folgenden Gründen keine regulären E-Mail-Nachrichten:

- Die E-Mail-Nachrichten könnten von einem Absender stammen, der in der Liste **Absender verweigern** aufgeführt ist. Sie müssen möglicherweise Folgendes durchführen:
  - Definieren Sie die Liste **Absender verweigern** genauer, um zu gewährleisten, dass erwünschte E-Mail-Nachrichten nicht blockiert werden. Es ist beispielsweise sinnvoller, eine bestimmte E-Mail-Adresse einzugeben, als eine gesamte Domäne oder ein gesamtes Netzwerk zu sperren.
  - Fügen Sie der Liste **Absender zulassen** den Absender, die Domäne oder das Netzwerk hinzu. Die Appliance scannt keine E-Mails von Absendern, Domänen und Netzwerken, die sich in dieser Liste befinden, auf Spam. Die Liste **Absender zulassen** hat Vorrang vor Einträgen in den Listen **Absender verweigern**.
- Die E-Mail-Nachricht wurde vielleicht blockiert, weil sie von einem Absender oder einem Unternehmen stammt, der bzw. das von einer Ihrer Echtzeit-Anti-Spam-Listen als potenzielle Spam-Quelle erkannt wurde.
- Das Verhältnis zwischen blockierten Spam- und regulären E-Mail-Nachrichten muss möglicherweise korrigiert werden. Wenn die Appliance beispielsweise selbst E-Mail-Nachrichten mit einem nur geringen Spam-Risiko blockiert, laufen Sie Gefahr, versehentlich auch normale

E-Mail-Nachrichten zu blockieren. Es ist sinnvoller, eine gewisse Anzahl von Spam-Mails zu riskieren.

- Die E-Mail-Nachricht könnte einen Virus oder ein potenziell unerwünschtes Programm enthalten und wurde durch einen Virenscanner blockiert.

Benutzer erhalten weiterhin Spam.

Benutzer empfangen möglicherweise aus folgenden Gründen weiterhin Spam:

- Keine Anti-Spam-Software kann alle E-Mail-Nachrichten blockieren, die Spam enthalten könnten. Um Spam bestmöglich zu erkennen und zu verhindern, vergewissern Sie sich, dass die Appliance die neuesten Versionen des Anti-Spam-Moduls, der Anti-Spam-Regeln und zusätzlicher Regeldateien sowie alle Funktionen verwendet, die unerwünschte E-Mails blockieren können.
- Die Appliance lässt das Passieren von Stream-Medien zu.

  HINWEIS: Das Passieren von Stream-Medien stellt ein Sicherheitsrisiko dar, da Stream-Medien nicht von der Appliance gescannt werden. McAfee rät davon ab, Stream-Medien des Typs *application/octet-stream oder application/** die Appliance passieren zu lassen, da diese MIME-Typen ausführbar sind und ein hohes Sicherheitsrisiko darstellen.

- Die Anti-Spam-Erkennung ist nicht auf der Appliance aktiviert. Die Scan-Vorgänge müssen für die korrekte Richtung aktiviert werden. Wenn Spam aus einer externen Quelle erkannt werden soll, aktivieren Sie den Spam-Scan für eingehenden Datenverkehr. Wenn Spam aus einer internen Quelle erkannt werden soll, aktivieren Sie den Spam-Scan für ausgehenden Datenverkehr.
- Sie müssen möglicherweise eine strengere Anti-Spam-Richtlinie einrichten. Möglicherweise möchten Sie z. B. mehr E-Mail-Nachrichten als Spam markieren, bevor diese von den Benutzern empfangen werden, oder einfach Spam auf der Appliance-Ebene blockieren.
- Die E-Mail-Nachrichten könnten von Absendern, Domänen oder Netzwerken stammen, die in der Liste **Absender zulassen** aufgeführt sind. Überprüfen Sie die Liste, um sicherzugehen, dass E-Mail-Nachrichten von diesen Absendern wirklich vom Anti-Spam-Scan ausgenommen werden sollen. Möglicherweise sollten Sie die Einträge der Liste genauer definieren. Geben Sie beispielsweise einzelne E-Mail-Adressen an, statt ganze Domänen oder Netzwerke zuzulassen.
- Die E-Mail-Client-Software verschiebt unerwünschte Nachrichten nicht automatisch in einen Spam-Ordner. Benutzer sehen also weiterhin Spam-Nachrichten in ihrem Posteingang.
- Die E-Mail-Nachricht könnte größer sein als zulässig, weshalb sie nicht auf Spam gescannt wird. Die Größe können Sie in Ihren erweiterten Einstellungen für Spam ändern.
- Die E-Mail-Nachrichten werden nicht über eine Appliance geroutet, auf der das Anti-Spam-Modul aktiviert ist.

Wie kann ein bestimmter Typ von Spam gestoppt werden?

Überprüfen Sie Folgendes, um die optimale Erkennung und Vermeidung von Spam sicherzustellen:

- Die Appliance nutzt die neuesten Versionen des Anti-Spam-Moduls und der Anti-Spam-Regeln.
- Die Appliance wurde so konfiguriert, dass Stream-Medien die Appliance nicht passieren können.

Warum hat sich die Leistung verschlechtert?

Für das Scannen von E-Mail-Nachrichten auf Spam werden Ressourcen der Appliance benötigt, wodurch die SMTP-Leistung beeinträchtigt wird.

Benutzer klagen über volle Posteingänge.

Wenn Benutzer Spam automatisch in einen Spam-Ordner im Posteingang umleiten, kann ihr Posteingang rasch sein Größenlimit überschreiten. Erinnern Sie die Benutzer daran, regelmäßig ihre Spam-Ordner zu überprüfen und Spam zu löschen.

Weitere Hilfe – Die Link-Leiste

Die Link-Leiste im Benutzeroberflächen-Fenster der Appliance bietet Links zu weiteren Informationsquellen. Sie haben folgende Möglichkeiten:

- Greifen Sie auf die Online-Virenbibliothek von McAfee zu, um mehr über einen bestimmten Virus herauszufinden.
- Senden Sie eine Virenprobe zur Analyse an McAfee.
- Setzen Sie sich mit dem Technischen Support von McAfee in Verbindung.

Weitere Informationen hierzu finden Sie in der *Online-Hilfe*.